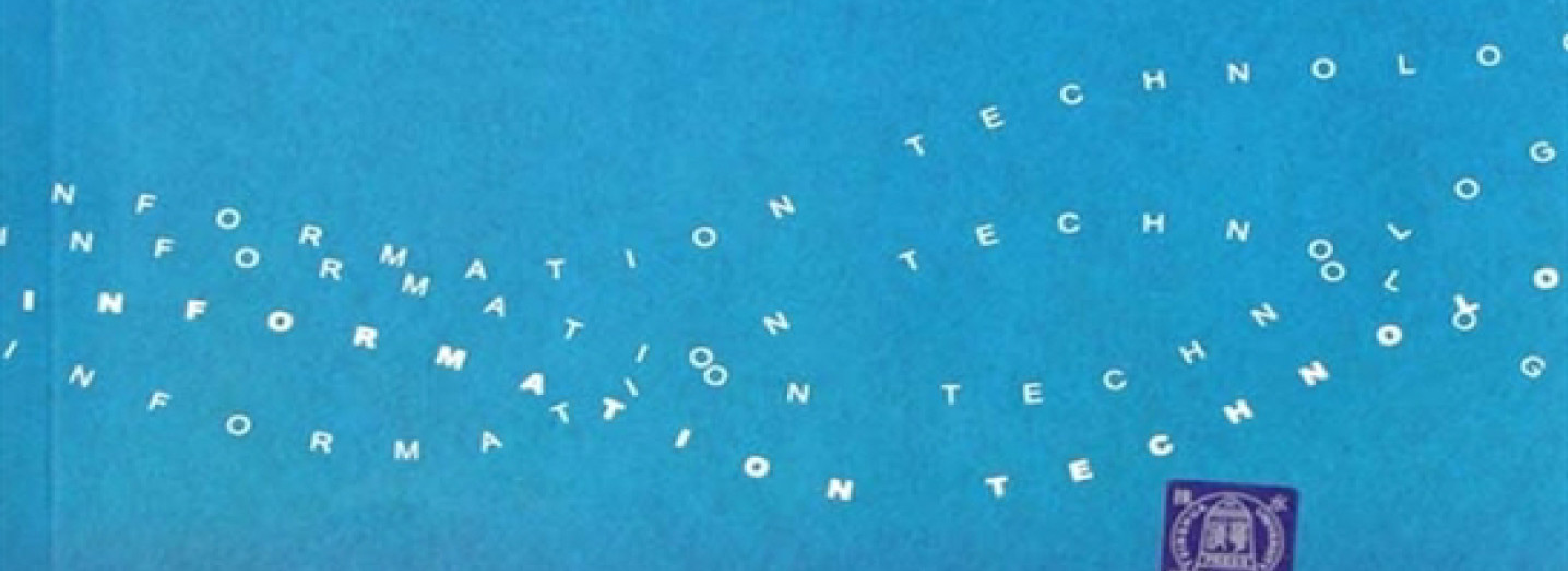
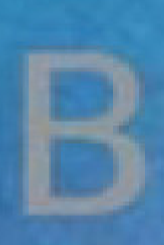
高等院校信息技术规划教材

计算机与网络安全实用技术

杨云江 编著



清华大学出版社



高等院校信息技术规划教材

计算机与网络安全
实 用 技 术

杨云江　编著

清 华 大 学 出 版 社

北　京

内容提要

本书从计算机安全的基本知识入手，全面介绍了计算机安全和计算机网络安全的基本原理、体系结构，并在对网络脆弱性分析的基础上，介绍了计算机网络安全的实施手段和安全管理技术。

本书的主要内容有计算机网络安全的基本概念、计算机环境安全技术、计算机系统安全与数据备份技术、信息安全技术、通信安全技术、局域网与 Internet 安全技术、网络操作系统安全技术、防火墙安全技术、入侵检测技术、端口扫描技术、嗅探技术、病毒诊断与病毒的防治技术、黑客攻击与黑客防范技术。

本书内容丰富、图文并茂，注重理论联系实际，书中附有大量实用工具的使用技术，能够很好地帮助读者学习和理解计算机网络安全管理技术。

本书可作为大专院校计算机、通信工程、电子科学技术及其相关学科和专业高年级本科、研究生的专业课教材，还可作为网络管理员和网络安全员的培训教材及网络工程与通信工程技术人员的参考书籍。

图书在版编目（CIP）数据

计算机与网络安全实用技术/杨云江编著. —北京：清华大学出版社，2007.8
（高等院校信息技术规划教材）
ISBN 978-7-302-15174-6

Ⅰ. 计…　Ⅱ. 杨…　Ⅲ. ①电子计算机－安全技术－高等学校－教材 ②计算机网络－安全技术－高等学校－教材　Ⅳ. TP309　TP393.08

中国版本图书馆 CIP 数据核字(2007)第 067693 号

责任编辑：袁勤勇　李　晔
责任校对：李建庄
责任印制：王秀菊

出版发行：清华大学出版社　　**地　　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编：**100084
社　总　机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印　刷　者：北京市昌平环球印刷厂
装　订　者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张：**21.75　　**字　数：**503 千字
版　　次：2007 年 8 月第 1 版　　**印　次：**2008 年 6 月第 2 次印刷
印　　数：3001～5000
定　　价：28.00 元

前言 foreword

当今世界是信息化的时代，信息已作为人类社会继人、财、物之后的第四大财富，随着人们对计算机网络的依赖日益增强，越来越多的信息和重要数据资源都出现在网络中，通过计算机网络获取信息的方式已成为人们信息沟通的主要方式，也是现代人类生活的重要组成部分。然而，人们在使用计算机网络获得诸多便利和好处的同时，也受到了来自黑客、计算机病毒的侵袭和威胁，使个人、家庭、单位乃至国家蒙受巨大的损失，特别是自20世纪90年代以来，随着Internet网络规模爆炸式的增长，网络上各种新业务（如电子政务、电子商务、网络银行和网上购物等）的兴起以及各种专用网络（如金融网、金税网和教育网等）的建设，使得如何保障信息安全及计算机网络安全已成为一个亟待解决的问题，计算机安全及网络安全也已成为当前的重要研究课题。

作者根据多年的教学经验和实践经验编写出了本书，旨在帮助广大读者全面了解和掌握计算机及网络安全的基本原理、结构、安全管理实施手段及管理技术。殷切希望本书的出版能给读者带来收益和帮助。

本书内容丰富、图文并茂，注重理论联系实际，书中列举了大量的应用实例，并介绍了大量网络安全管理实用工具的使用技术，如常用扫描工具、常用病毒的诊断与清除技术以及常用嗅探器的使用技术。

本书共13章，第1章介绍计算机安全与网络安全的基本概念，第2章介绍计算机环境安全技术，第3章介绍计算机系统安全与数据备份技术，第4章介绍信息安全技术，第5章介绍网络通信安全技术，第6章介绍局域网与Internet安全技术，第7章介绍网络操作系统的安全技术，第8章介绍防火墙及其安全技术，第9章介绍网络入侵检测技术，第10章介绍端口及漏洞扫描技术，第11章介绍嗅探原理及嗅探技术，第12章介绍计算机病毒诊断与防范技术，第13章介绍黑客的常用攻击手段及黑客防范技术。

在编写本书的过程中，作者借鉴和参考了许多有关计算机安

全、信息安全及网络安全的书籍和文章，并参考了许多网站资料，在此向有关作者表示谢意。

由于作者水平有限，加上时间匆忙，书中难免有错误和疏漏之处，恳请广大读者批评指正，不胜感谢。

杨云江

2007 年 6 月

目录 Contents

第 1 章 chapter 1

计算机安全与网络安全概论

在当今信息化的社会中，人们对计算机网络的依赖日益增强，越来越多的信息和重要数据资源出现在网络中。通过网络获取信息的方式已成为当前主要的信息沟通方式之一，这种趋势还在不断地发展。人们在使用 Internet 获得诸多便利和好处的同时，也受到了来自黑客、计算机病毒的侵袭和威胁，使个人和单位蒙受了巨大的损失，特别是近年来 Internet 呈规模爆炸式的增长，网络上各种新业务（如电子政务、电子商务、网络银行和网上购物等）的兴起以及各种专用网络（如金融网、金税网和教育网等）的建设，使得如何保障计算机安全及网络安全已成为目前一个亟待解决的问题。因此，计算机安全及网络安全技术成为当前网络技术的重要研究课题和发展方向。

计算机安全及网络安全主要的研究内容如下：

- 计算机环境安全技术。
- 计算机硬件安全技术。
- 计算机软件安全技术。
- 数据备份与信息安全技术。
- 网络平台安全技术。
- 网络通信安全技术。
- 网络操作系统安全技术。
- 防火墙技术。
- 入侵检测与端口扫描技术。
- 计算机病毒与黑客的防范技术。

本书将对上述内容逐步加以介绍。

本章着重介绍计算机网络安全的基础知识，并对计算机网络安全问题的基本内容进行介绍。

1.1 计算机安全与网络安全

1.1.1 信息安全

1. 信息安全的基本概念

在这里，给信息安全下一个定义：

国际标准化组织(ISO)对信息安全的定义为：为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。

我国安全保护条例对信息安全的定义为：计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

可以把信息安全保密内容分为实体安全、运行安全、数据安全和管理安全4个方面。

计算机信息系统安全的目标是着力于实体安全、运行安全、信息安全和人员安全。安全保护的直接对象是计算机信息系统，实现安全保护的关键因素是人。

信息安全主要涉及到信息传输的安全、信息存储的安全以及对网络传输信息内容的审计3方面。

1) 信息传输安全系统

- 信息传输加密技术。目的是对传输中的数据流加密，以防止通信线路上的窃听、泄漏、篡改和破坏。如果以加密实现的通信层次来区分，加密可以在通信的三个不同层次来实现，即链路加密(位于OSI网络层以下的加密)、结点加密和端到端加密(传输前对文件加密，位于OSI网络层以上的加密)。

一般常用的是链路加密和端到端加密这两种方式。链路加密侧重在通信链路上而不考虑信源和信宿，是对保密信息通过各链路采用不同的加密密钥提供安全保护。链路加密是面向结点的，对于网络高层主体是透明的，它对高层的协议信息(地址、检错及帧头帧尾)都加密，因此数据在传输中是密文，但在中央结点必须解密得到路由信息。端到端加密则指信息由发送端自动加密，并进入TCP/IP数据包封装，然后作为不可阅读和不可识别的数据穿过互联网，当这些信息一旦到达目的地，将自动重组、解密，成为可读数据。端到端加密是面向网络高层主体的，它不对下层协议进行信息加密，协议信息以明文形式传输，用户数据在中央结点不需解密。

- 数据完整性鉴别技术。目前，对于动态传输的信息，许多协议确保信息完整性的方法大多是收错重传、丢弃后续包的办法，但黑客的攻击可以改变信息包内部的内容，所以应采取有效的措施来进行完整性检验控制。
- 报文鉴别。与数据链路层的循环冗余校验(Cyclic Redundancy Check，CRC)控制类似，将报文名字段(或域)使用一定的操作组成一个约束值，称为该报文的完整性检测向量(Integrated Check Vector，ICV)。然后将它与数据封装在一起进行加密，传输过程中由于侵入者不能对报文解密，所以也就不能同时修改数据并计算新的ICV，这样，接收方收到数据后解密并计算ICV，若与明文中的ICV不同，则认为此报文无效。
- 校验和。一个最简单易行的完整性控制方法是使用校验和，计算出该文件的校验和值并与上次计算出的值比较。若相等，说明文件没有改变；若不等，则说明文件可能被未察觉的行为改变了。校验和方式可以查错，但不能保护数据。
- 加密校验和。将文件分成小块，对每一块计算CRC校验值，然后再将这些CRC值加起来作为校验和。只要运用恰当的算法，这种完整性控制机制几乎无法破

解。但这种机制运算量大,并且昂贵,只适用于那些完整性要求保护极高的情况。

- 消息完整性编码(Message Integrity Code,MIC)。使用简单单向散列函数计算消息的摘要,连同信息发送给接收方,接收方重新计算摘要,并进行比较验证信息在传输过程中的完整性。这种散列函数的特点是任何两个不同的输入不可能产生两个相同的输出。因此,一个被修改的文件不可能有同样的散列值。单向散列函数能够在不同的系统中高效实现。
- 防抵赖技术。它包括对源和目的地双方的证明,常用方法是数字签名,数字签名采用一定的数据交换协议,使得通信双方能够满足两个条件,接收方能够鉴别发送方所宣称的身份,发送方事后不能否认他发送过数据这一事实。比如,通信的双方采用公钥体制,发送方使用接收方的公钥和自己的私钥加密的信息,只有接收方凭借自己的私钥和发送方的公钥解密之后才能读懂,而对于接收方的回执也是同样道理。另外实现防抵赖的途径还有通过可信第三方的认证、使用时间戳、采用一个在线的第三方、数字签名与时间戳相结合等。

鉴于为保障数据传输的安全,需采用数据传输加密技术、数据完整性鉴别技术及防抵赖技术。因此为节省投资、简化系统配置、便于管理、使用方便,有必要选取集成的安全保密技术措施及设备。这种设备应能够为大型网络系统的主机或重点服务器提供加密服务,为应用系统提供安全性强的数字签名和自动密钥分配功能,支持多种单向散列函数和校验码算法,以实现对数据完整性的鉴别。

2) 信息存储安全系统

在计算机信息系统中存储的信息主要包括纯粹的数据信息和各种功能文件信息两大类。对纯粹数据信息的安全保护,以数据库信息的保护最为典型。而对各种功能文件的保护,终端安全很重要。

(1) 数据库安全。

对数据库系统所管理的数据和资源提供安全保护,其安全功能如下:

- 物理完整性。即数据能够免于物理方面破坏的问题,如掉电、火灾等。
- 逻辑完整性。能够保持数据库的结构,比如对一个字段的修改不至于影响其他字段。
- 元素完整性。包括在每个元素中的数据是准确的。
- 数据的加密。数据以密文形式存储和传输,需要时再进行解密。
- 用户鉴别。确保每个用户被正确识别,避免非法用户入侵。
- 可获得性。指用户一般可访问数据库和所有授权访问的数据。
- 可审计性。能够追踪到谁访问过数据库。

要实现对数据库的安全保护,一种选择是安全数据库系统,即系统的设计、实现、使用和管理等各个阶段都要遵循一套完整的系统安全策略;二是以现有数据库系统所提供的功能为基础构建安全模型,旨在增强现有数据库系统的安全性。

(2) 终端安全。

主要解决计算机终端信息的安全保护问题,其安全功能如下:

- 基于口令密码算法的身份验证,防止非法使用机器。

- 自主和强制存取控制，防止非法访问文件。
- 多级权限管理，防止越权操作。
- 存储设备安全管理，防止非法软盘复制和硬盘启动。
- 数据和程序代码加密存储，防止信息被窃。
- 预防病毒，防止病毒侵袭。
- 严格的审计跟踪，便于追查责任事故。

3）信息内容审计系统

实时对进出内部网络的信息进行审计，以防止或追查可能的泄密行为。因此，为了满足国家保密法的要求，在某些重要或涉密网络，应该安装使用审计系统。

2. 信息安全的特点

- 相对性。没有绝对的安全，只有相对的安全。其安全程度与面临的安全风险大小、安全防护人力、物力投入多少相关。
- 综合性。信息安全并非一个单纯的技术层面的问题，它还涉及到管理、意识和国家法律等多个层面，因此，信息安全其实是一个综合性的问题，各个环节紧密衔接在一起。
- 产品多样性。防黑客的产品不能用来防病毒，不同强度控制不同风险，不能仅指望靠单一的网络安全产品来做到一劳永逸。
- 动态性。今天安全不等于明天就安全，在前一段时间看来是较为安全的问题随着黑客技术的发展也会暴露出原来未检测到的漏洞，所以需要对黑客行为模式进行不断提炼，在技术上的及时跟进和维护支持非常重要。
- 不易管理性。显然安全保护越好，就越不易于管理，而我们不能限制网络带来的优势，因此投资、安全和便捷之间需要平衡，通过将不同技术控制手段和管理的结合来实现。
- 黑盒性。信息与网络的不安全性是相对透明的，也就是说，信息安全与网络安全是具有黑盒性的。信息安全与网络安全工具和设备在运行时对用户是不可见的，到底能防多少黑客、系统受多少伤害、是否带来新的不安全因素，包括整个安全体系都是很模糊的，用户不知如何管理，本书将提到的网络安全资源管理平台就可以给管理人员一片感性的天地。

3. 信息安全的三个层面

信息安全是要保证信息的完整性、可用性和保密性。当前，信息安全可以分为 3 个层面：网络安全、系统安全以及信息数据安全。

网络层安全问题的核心在于网络是否得到控制，一旦危险的访问者进入企业网络，后果是不堪设想的。这就要求网络能够对所有来访者进行分析，判断来自这一 IP 地址的数据是否安全，以及是否会对本网络造成危害；同时还要求系统能自动将危险来访拒之门外，并对其进行自动记录，使其无法再次入侵。

系统层面的安全问题，主要是病毒对于网络的威胁。病毒的危害已是人尽皆知了，

它就像是暗藏在网络中的不定时炸弹，系统随时都有可能遭到破坏而导致严重后果甚至造成系统瘫痪。因此企业必须做到实时监测，随时查毒、杀毒，不能有丝毫的懈怠与疏忽。

信息数据是安全问题的关键，要求保证信息传输的完整性、保密性等。这一安全问题所涉及的是使用系统中的资源和数据的用户是否是真正被授权的用户，这就要求系统能够对网络中流通的数据信息进行监测、记录，并对使用该系统信息数据的用户进行身份认证，以保证信息安全。

目前，针对这 3 个层面而开发出的信息安全产品主要包括杀毒软件、防火墙、安全管理、认证授权和加密等。其中以杀毒软件和防火墙应用最为广泛。

1.1.2 计算机安全

1. 计算机安全的基本概念

1946 年，计算机问世的初期，人们关注的是如何提高计算机的计算处理能力、运算速度和存储能力，并没有过多地考虑到计算机安全的问题。以后，随着多用户、多进程计算机的出现，众多用户使用同一台计算机运行不同的进程，由此产生了计算机账户管理和资源分配等需求，因此出现了身份认证和访问控制，开始在操作系统中设置专门的用户口令文件和用户账户文件，并在用户登录时引发身份认证进程。计算机还为不同的用户设置专用目录和公用目录，根据预先分配用户的权限来控制其访问范围。从而引入了计算机安全的概念，20 世纪 70 年代初出现的 UNIX 操作系统就具备了这样的安全机制。实质上，计算机安全是研究如何预防和检测计算机系统用户的非授权行为。

计算机安全是以信息安全为基础的，也即是以信息的存储、访问、传输的安全为宗旨的安全机制。将在后面的内容中介绍。

2. 计算机安全的基本内容

计算机安全主要分为 3 大部分：硬件安全、软件安全及数据安全。

硬件安全主要是指计算机及其外围设备的安全，尤其是存储设备的安全显得最为重要。因为在计算机中，诸多的重要数据（比如个人隐私、企业营销信息和国家机密等），都是存放在存储设备上的，一旦这些存储设备遭到攻击或破坏，后果是不堪设想的。

计算机系统硬件安全有两个含义，其一是保护硬件系统免遭攻击，其二是保护硬件系统免遭破坏。前者指的是如何防止系统遭到攻击，后者指的是对于一旦硬件遭到攻击后，如何恢复原有数据的问题。

软件安全指的是对各种应用软件进行访问权限的设置，没有授权的用户是不能访问该软件的。

数据安全指的是对数据的存储、访问、传输的保密与安全。

数据的存储安全类似于计算机硬件安全，其一是保护数据免遭攻击，其二是保护数据免遭破坏，其三是对数据进行加密。

数据的访问安全指的是对用户设置数据的访问权限，不同权限的用户的访问范围是

不一样的，对于没有权限的用户，是不能随意访问数据的。

数据的传输安全指的是保护数据在传输过程中免遭窃听、窃取、篡改和破坏。

后面将要介绍，计算机安全是以信息安全为基础的，也即是以信息的存储、访问和传输的安全为宗旨的安全机制。

1.1.3 网络安全

1. 网络安全管理的意义

随着人类社会生活对 Internet 需求的日益增长，网络安全逐渐成为 Internet 及各项网络服务和应用进一步发展的关键问题，特别是 1993 年以后 Internet 开始商用，通过 Internet 进行的各种电子商务业务日益增多，加之 Internet/Intranet 技术日趋成熟，很多组织和企业都建立了自己的内部网络并与 Internet 连接。电子商务应用和企业网络中的商业秘密均成为攻击者的目标。

随着 Internet 的发展，网络安全技术也在与网络攻击的对抗中不断发展。从总体上看，经历了从静态到动态、从被动防范到主动防范的发展过程。计算机网络安全是一个非常复杂的问题，安全问题不仅仅是技术方面的问题，它还涉及人的心理、社会环境以及法律等多方面内容。

在计算机网络系统中，多个用户共处在一个大环境中，系统资源是共享的，用户终端可直接访问网络和分布在各用户处理机中的文件、数据和各种软件、硬件资源。随着计算机和网络的普及，政府、军队的核心机密和重要数据、企业的商业机密、甚至是个人的隐私都存储在计算机网络中，不法之徒千方百计的“闯入”和破坏，使有关方面蒙受了巨大的损失。

综上所述，网络安全技术主要用于保证网络环境中各种应用系统和信息资源的安全，防止未经授权的用户非法登录系统，非法访问网络资源，窃取信息或实施破坏。网络系统安全主要侧重于攻击行为和特征的检测和阻断、系统防护和灾难恢复方面的研究。主要技术有防火墙、访问控制、入侵检测、漏洞扫描、身份认证、灾难恢复和安全管理等。

2. 计算机网络安全的有关概念

- 安全与保密。计算机网络安全是指网络系统中用户共享的软、硬件等各种资源是否安全，使其不受到有意无意的破坏，不被非法入侵等。研究计算机网络安全问题必然要涉及到保密问题，但安全与保密却不是等同的两个概念。在研究网络安全问题时，针对非法侵入、盗窃机密等方面的安全问题要用保密技术加以解决。保密是指为维护用户自身利益，对资源加以防止非法侵入和防止盗取，即使非法用户盗取到了资源也识别不了的方法。
- 风险与威胁。风险是指损失的程度，威胁是指对资产构成威胁的人、物、事及想法。其中资产是进行风险分析的核心内容，它是系统必须保护的，网络系统中的资产主要是数据。威胁会利用系统所暴露出的弱点和要害之处对系统进行攻击，威胁包括有意和无意两种。

• 敏感信息。敏感信息是指那些丢失、滥用、被非法授权人访问或修改的信息，是泄露、破坏、不可使用或修改后会对你造成损失的信息。
• 脆弱性。脆弱性是指在系统中安全防护的弱点或缺少用于防止某些威胁的安全防护。脆弱性与威胁是密切相关的。
• 控制。控制是指为降低受破坏可能性所做的努力。

3. 安全管理的基本内容

安全管理包括安全特征的管理和管理信息的安全。

安全特征的管理提供安全的服务，以及安全机制变化的控制，直至物理场地、人员的安全，病毒防范措施操作过程的连续性，灾难事故时恢复措施的计划与实施等内容，管理信息的安全是保障管理信息自身的安全。安全管理提供的主要功能包括：

• 安全告警管理。
• 安全审计跟踪功能管理。
• 安全访问控制管理。

4. 保护网络系统的基本要素

1）安全策略

制定对系统进行有效管理的安全策略。网络系统的安全策略包括下述内容：

• 使用口令登录进行访问控制。
• 制定网络操作系统和用户应用程序的安全控制。
• 对付系统备份、灾难系统和数据恢复的安全机制。
• 网络系统的重要资源(如服务器、路由器、交换机和软件等)的物理安全策略。
• 明确网络安装和维护的软件硬件人员的职责及网络访问级别。
• 在进行网络外部访问时维护网络完整性的策略。

2）防火墙

将非法信息和非法入侵人员挡在“墙外”的一种技术。

在计算机网络系统中，“防火墙”是用来限制和隔离网络用户的某些工作的一种特殊技术，安全系统对外来造访者可以通过防火墙技术来实现安全保护。

防火墙实质上是用“包过滤”技术来实现的，将对内部网络造成威胁或危害的外来“数据包”挡在墙外。

3）记录

将网络运行情况详细记录下来，以便事后进行分析。

系统必须能自动记录网上的每项活动，系统管理员则采取一些特殊手段对这些记录信息进行处理，以便获得所需信息来定位和特征化入侵行为。

4）脆弱性评价

详细分析系统的脆弱性，及时改进。

5）物理保护

物理保护指的是对计算机网络的物理设备和通信介质进行有效的保护。主要防止

搭线窃取网络数据。

6）注册登录

注册登录的限制。

1.2 计算机网络面临的安全问题

1.2.1 网络脆弱性分析

计算机网络尤其是互联网络，由于网络分布的广域性、网络体系结构的开放性、信息资源的共享性和通信信道的共用性，而使计算机网络存在严重的脆弱点。它们是网络安全的隐患。给攻击型的威胁提供了可乘之机，对于网络安全来说，找到和确认这些脆弱点是至关重要的。

1. 网络漏洞

不设防的网络会有成百上千个漏洞和后门。机器设备、计算机硬件和软件、网络系统，甚至有些安全产品本身就存在安全漏洞。

2. 电磁辐射

电子设备工作过程都有电磁辐射产生。电磁辐射在网络中表现出两方面的脆弱性。一方面，电磁辐射能够破坏网络中传输的数据，这种辐射的来源有两个方面，网络周围电子电气设备产生的电磁辐射和试图破坏数据传输而预谋的干扰辐射源；另一方面，网络的终端、打印机或其他电子设备在工作时产生的电磁辐射泄露，即使用不太先进的设备，在近处甚至远处都可以将这些数据，包括在终端屏幕上显示的数据接收下来，并且重新恢复。

3. 线路窃听

无源线路窃听通常是一种没有检测的窃听，它通常是为了获取网络中的信息内容。有源线路窃听是对信息流进行有目的的变形，能够任意改变信息内容，注入伪造信息，删除和重发原来的信息。也可以用于模仿合法用户，或通过干扰阻止和破坏信息传输。

4. 串音干扰

串音的作用是产生传输噪音，噪音能对网络上传输的信号造成严重的破坏。

5. 硬件故障

硬件故障势必造成软件中断和通信中断，带来重大损害。

6. 软件故障

通信网络软件一般用于建立计算机和网络的连接。程序里包含有大量的管理系统



安全的部分，如果这些软件程序受到损害，则该系统就是一个极不安全的系统。

7. 人为因素

系统内部人员的非法活动，如系统操作员、工程技术人员和管理人员盗窃机密数据或破坏系统资源。利用制度不健全或管理不严盗窃存有机密数据的媒体，甚至直接破坏网络系统。

8. 网络规模

网络安全的脆弱性和网络的规模有密切关系。网络规模越大，其安全的脆弱性越大。资源共享与网络安全也是矛盾的，随着网络发展和资源共享增强，安全问题也越突出。

9. 网络物理环境

这种类型脆弱性是属于计算机设备防止自然灾害的领域，比如火灾和洪水。也包括一般的物理环境的保护，像机房的安全门、人员出入机房的规定等。物理环境安全保护的范围不仅包括计算机设备和传输线路，也包括一切可以移动的物品，比如打印数据的打印纸和装有数据和程序的磁盘。

10. 通信系统

通信系统始终是最严重的脆弱性课题。对于一般的通信系统，获得存取权是相对简单的，并且机会总是存在的。一旦信息从生成和存储的设备发送出去，它将给攻击型的威胁提供了巨大的突破口。

1.2.2 网络面临的威胁

网络安全潜在威胁形形色色，有人为和非人为的、恶意的和非恶意的、内部攻击和外部攻击等。对网络安全的威胁主要表现在非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒和线路窃听等方面。安全威胁主要利用以下途径，系统存在的漏洞；系统安全体系的缺陷；使用人员的安全意识薄弱；管理制度的不健全。

安全威胁可分为故意的（如系统入侵）和偶然的（如将信息发到错误地址）两类。故意威胁又可进一步分成被动威胁和主动威胁两类，被动威胁只对信息进行监听和窃取，而不对其修改和破坏；主动威胁则要对信息进行故意篡改和破坏，使合法用户得不到可用信息。网络安全主要有以下几种：

1. 基本的安全威胁

网络安全具备4个方面的特征，即机密性、完整性、可用性及可控性。下面的4个基本安全威胁直接针对这4个安全目标。

- 信息泄露。信息泄露给某个未经授权的实体。这种威胁主要来自窃听、搭线等信

息探测攻击。

- 完整性破坏。数据的一致性由于受到未授权的修改、创建、破坏而损害。
- 拒绝服务。对资源的合法访问被阻断。拒绝服务可能由以下原因造成,攻击者对系统进行大量的、反复的非法访问尝试而造成系统资源过载,无法为合法用户提供服务;系统物理或逻辑上受到破坏而中断服务。
- 非法使用。某一资源被非授权人以授权方式使用。

2. 主要渗入威胁

- 假冒。即某个实体假装成另外一个不同的实体。这个未授权实体以一定的方式使安全守卫者相信它是一个合法实体,从而获得合法实体对资源的访问权限。这是大多数黑客常用的攻击方法。如甲和乙同为网络上的合法用户,网络能为他们服务。丙也想获得这些服务,于是丙向网络发出:“我是乙”。
- 篡改。乙给甲发了如下一份报文:“请给丁汇 10000 元钱,乙”。报文在转发过程中经过丙,丙把报文改为“请给丙汇 10000 元钱,乙”。结果是丙而不是丁收到了这 10000 元钱。这就是报文篡改。
- 旁路。攻击者通过各种手段发现一些系统安全缺陷,并利用这些安全缺陷绕过系统防线渗入到系统内部。
- 授权侵犯。对某一资源具有一定权限的实体,将此权限用于未被授权的实体,也称“内部威胁”。

3. 主要植入威胁

- 计算机病毒。计算机病毒是一种会“传染”其他计算机程序并具有破坏能力的程序,“传染”是通过修改其他程序来把自身复制进去完成的。比如“特洛伊木马(Trojan horse)”,是一种执行超出程序定义之外的程序,如一个编译程序除了执行编译任务以外,还把用户的源程序偷偷地复制下来,这种编辑程序就是一个特洛伊木马。
- 陷门。在某个系统或某个文件中预先设置“机关”,诱你掉入“陷门”之中,一旦你提供特定的输入时,允许你违反安全策略,将自己机器上的秘密自动传送到对方的计算机上。

典型的安全威胁如表 1-1 所示。

表 1-1　典型的网络安全威胁

威　　胁	描　　　　述
授权侵犯	为某一特定目的被授权使用某个系统的人,将该系统用作其他未受权的目的
窃听	在监视通信的过程中获得信息
电磁泄露	从设备发出的辐射中泄露信息
信息泄露	信息泄露给未授权实体

续表

威　　胁	描　　　述
物理入侵	入侵者绕过物理控制而获得对系统的访问权
重放	出于非法目的而重新发送截获的合法通信数据
资源耗尽	某一资源被故意超负荷使用,导致其他用户的服务中断
完整性破坏	对数据的未授权创建、修改或破坏造成一致性损坏
人员疏忽	一个授权人出于某种动机或由于粗心将信息泄露给未授权的人

1.2.3　网络安全的基本技术

网络安全是对付威胁、克服脆弱性及保护网络资源的所有措施的总称,涉及政策、法律、管理、教育和技术等方面的内容。网络安全是一项系统工程,针对来自不同方面的安全威胁,需要采取不同的安全对策。从法律、制度、管理和技术上采取综合措施,以便相互补充,达到较好的安全效果。技术措施是最直接的屏障,目前常用而有效的网络安全技术对策有如下几种:

1. 数据加密技术

加密是所有信息保护技术措施中最古老、最基本的一种手段。加密的主要目的是防止信息的非授权泄漏。加密方法多种多样,在信息网络中一般是利用信息变换规则把可读的信息变成不可读的信息。既可对传输信息加密,也可对存储信息加密,把计算机数据变成一堆乱码数据。现代密码算法不仅可以实现加密,还可以实现数字签名、身份认证和报文完整性鉴别等功能,能有效地对抗截获、非法访问、破坏信息的完整性、冒充、抵赖和重放等威胁,因此,密码技术是信息网络安全的核心技术。

2. 数字签名技术

数字签名机制提供了一种鉴别方法,以解决伪造、抵赖、冒充和篡改等安全问题。数字签名采用一种数据交换协议,使得数据的收发双方能够满足三个条件,接受方能够鉴别发送方所宣称的身份;发送方事后不能否认他发送过数据这一事实;接收方事后不能伪造数字签名。数字签名一般采用非对称加密技术,发送方对整个明文进行加密变换,得到一个值,将其作为签名。接收者使用发送者的公开密钥对签名进行解密运算,如其结果为对方身份,则签名有效,证明对方身份是真实的。

3. 鉴别技术

鉴别的目的是验明用户或信息的正身。对实体声称的身份进行唯一地识别,以便验证其访问请求或保证信息来自或到达指定的源和目的。鉴别技术可以验证消息的完整性,有效地对抗冒充、非法访问、重放等威胁。按照鉴别对象的不同,鉴别技术可以分为消息源鉴别和通信双方相互鉴别;按照鉴别内容的不同,鉴别技术可以分为用户身份鉴

别和消息内容鉴别。鉴别的方法很多，利用鉴别码验证消息的完整性；利用通行字、密钥、访问控制机制等鉴别用户身份，防止冒充、非法访问。当今最佳的鉴别方法是数字签名，利用单方数字签名，可实现消息源鉴别、访问身份鉴别、消息完整性鉴别。利用收发双方数字签名，可同时实现收发双方身份鉴别、消息完整性鉴别。

4. 访问控制技术

访问控制的目的是防止非法访问。访问控制是采取各种措施保证系统资源不被非法访问和使用。一般采用基于资源的集中式控制、基于源和目的地址的过滤管理以及网络签证技术等技术来实现。

5. 安全审计技术

计算机安全审计是通过一定的策略，利用记录和分析历史操作事件发现系统的漏洞并改进系统的性能和安全。

6. 防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互连环境中。在大型网络系统与因特网互连的第一道屏障就是防火墙。防火墙通过控制和监测网络之间的信息交换和访问行为来实现对网络安全的有效管理，其基本功能为过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止行为；记录通过防火墙的信息内容和活动；对网络攻击进行检测和告警。

7. 入侵检测技术

网络入侵检测技术也叫网络实时监控技术，它通过硬件或软件对网络上的数据流进行实时检查，并与系统中的入侵特征数据库进行比较，一旦发现有被攻击的迹象，立刻根据用户所定义的动作做出反应，如切断网络连接，或通知防火墙系统对访问控制策略进行调整，将入侵的数据包过滤掉等。

通过入侵检测技术，可监视登录到系统用户的一切行为，当用户试图对系统造成安全威胁时，自动发出报警或切断网络。

8. 端口扫描技术

网络安全扫描技术是为使系统管理员能够及时了解系统中存在的安全漏洞，并采取相应防范措施，从而降低系统的安全风险而发展起来的一种安全技术。利用安全扫描技术，可以对局域网络、Web 站点、主机操作系统、系统服务以及防火墙系统的安全漏洞进行扫描，系统管理员可以了解在运行的网络系统中存在不安全的网络服务，在操作系统上存在可能导致遭受缓冲区溢出攻击或者拒绝服务攻击的安全漏洞，还可以检测主机系统中是否被安装了窃听程序，防火墙系统是否存在安全漏洞和配置错误等。

9. 网络嗅探技术

网络嗅探是利用计算机的网络接口截获目的地及其他计算机数据报文的一种技术。它工作在网络的最底层,把网络传输的全部数据记录下来。以帮助网络管理员查找网络漏洞和检测网络性能,还可以分析网络的流量,以便找出所关心的网络中潜在的问题。

10. 病毒诊断与防治技术

病毒对计算机及网络造成的威胁是极大的,一个安全的计算机网络系统,必须要有强大的病毒诊断能力和防范措施。

11. 黑客防范技术

"黑客"就是非法入侵者,他对计算机网络的威胁也是不可估量的。黑客的防范技术有防火墙技术、口令保护技术、"堡垒主机"技术和"蜜罐"技术。

1.2.4 网络安全的基本功能

一个安全的计算机网络系统,通常是由下列功能组成的。

1. 身份识别

身份识别是安全系统应具备的最基本功能。这是验证通信双方身份的有效手段。用户向其系统服务时,要出示自己的身份证明。例如在进入一个系统或进程时,需要提交 User ID(用户名)和 Password(口令)。系统应具备检查用户身份的能力,对于用户的输入,能够明确判别该输入是否来自合法用户。

2. 存取权限控制

存取权限的基本任务是,防止非法用户进入系统及防止合法用户对资源的非法使用。在开放系统中,网上资源的使用应制定一些规定:一是定义哪些用户可以访问哪些资源;二是定义可以访问的用户各自具备的读、写操作等权限。

3. 保护数据完整性

主要通过消息摘要算法保护数据的完整性。

4. 审计追踪

通过系统日志记录的数据,对一些关键数据进行统计分析,当系统出现安全问题时能够追查原因。

5. 密钥管理

密钥安全管理有两方面的含义:一是对密钥的产生、存储、传送和定期更换进行有效地控制并引入密钥管理机制;二是对密钥进行加密,即是要求密钥必须经加密处理后方

能允许通过公共网络(如 Internet)进行传播。

1.3 系统安全策略

在规划和建设一个网络之前,必须要明确哪些资源、服务类型需要保护,并要求明确其保护的重要程度和防护对象,这就是所谓的安全策略。安全策略是由一组规则组成的,是对系统中所有与安全相关元素的活动做出的一些限制。

由于系统安全是由信息安全、计算机安全和网络安全组成的,在本节中,将依次介绍这 3 个方面的安全策略,其中重点是网络安全策略。

1.3.1 信息安全策略

1. 信息安全策略的定义

信息安全策略是一组规则,它们定义了一个组织要实现的安全目标和实现这些安全目标的途径。信息安全策略可以划分为两个部分,问题策略(issue policy)和功能策略(functional policy)。问题策略描述了一个组织所关心的安全领域和对这些领域内安全问题的基本态度。功能策略描述如何解决所关心的问题,包括制定具体的硬件和软件配置规格说明、使用策略以及雇员行为策略。信息安全策略必须有清晰和完全的文档描述,必须有相应的措施保证信息安全策略得到强制执行。在组织内部,必须有行政措施保证既定的信息安全策略被不打折扣地执行,管理层不能允许任何违反组织信息安全策略的行为存在,另一方面,也需要根据业务情况的变化不断地修改和补充信息安全策略。

2. 信息安全策略框架

信息安全策略框架包括以下内容:

- 加密策略。描述组织对数据加密的安全要求。
- 使用策略。描述设备使用、计算机服务使用和雇员安全规定、以保护组织的信息和资源安全。
- 线路连接策略。描述诸如传真发送和接收、模拟线路与计算机连接、拨号连接等安全要求。
- 反病毒策略。给出有效减少计算机病毒对组织威胁的一些指导方针,明确在哪些环节必须进行病毒检测。
- 应用服务策略。定义应用服务提供者必须遵守的安全方针。
- 审计策略。描述信息审计要求,包括审计小组的组成、权限、事故调查、安全风险估计、信息安全策略符合程度评价、对用户和系统活动进行监控等活动的要求。
- 电子邮件使用策略。描述内部和外部电子邮件接收、传递的安全要求。
- 数据库策略。描述存储、检索和更新等管理数据库数据的安全要求。
- 非军事区域策略。定义位于“非军事区域”(demilitarized zone)的设备和网络分区。

- 第三方的连接策略。定义第三方接入的安全要求。
- 敏感信息策略。对于组织的机密信息进行分级，按照它们的敏感度描述安全要求。
- 内部策略。描述对组织内部的各种活动安全要求，使组织的产品服务和利益受到充分保护。
- Internet 接入策略。定义在组织防火墙之外的设备和操作的安全要求。
- 口令防护策略。定义创建，保护和改变口令的要求。
- 远程访问策略。定义从外部主机或者网络连接到组织的网络进行外部访问的安全要求。
- 路由器安全策略。定义组织内部路由器和交换机的安全配置。
- 服务器安全策略。定义组织内部服务器的安全配置。
- VPN 安全策略。定义通过 VPN 接入的安全要求。
- 无线通信策略。定义无线系统接入的安全要求。

1.3.2 计算机安全策略

计算机安全策略主要研究的是如何预防和检测计算机系统用户的非授权行为。换句话说，计算机安全是关于对信息和资源的控制访问。

1. 计算机安全的结构

一个完整的计算机系统是由计算机硬件、软件、应用程序、资源（主体）和用户（客体）组成的。在这里，将用二维空间结构图来描述计算机安全的结构，如图 1-1 所示。

在图 1-1 中，横轴代表安全策略的重点，纵轴代表具有保护机制的计算机系统层次。

图 1-1 计算机安全结构图

2. 控制重点

计算机安全的重点是保证数据的完整性策略，可以用下列规则进行描述。

- 数据项的格式和内容。比如，一条规则可以规定账目数据库中的余额域必须包括一个整数（典型的实例是，银行活期存款中规定一张存折的余额不能小于 1 元）。这个规则并不依赖于访问数据项的用户或者作用在数据项上的操作。
- 规定作用在一个数据项上所有可能的操作。比如，一条规则可以规定只有开户、查询余额、取款和存款操作，可以访问账目数据库中的余额项，并且只有银行工作人员允许执行“开户”操作。
- 规定访问一个数据项的用户。比如，一条规则可以规定只有账户的持有者和银行工作人员才可以访问账目数据库。

由此可以得到一个结论，计算机系统的安全保护策略是保护计算机操作系统和数据的安全。

3. 计算机系统的保护机制

一个完整的计算机系统应由硬件、操作系统、服务、应用程序和外围环境组成。可以将其保护机制想象成一个个同心圆，如图 1-2 所示。

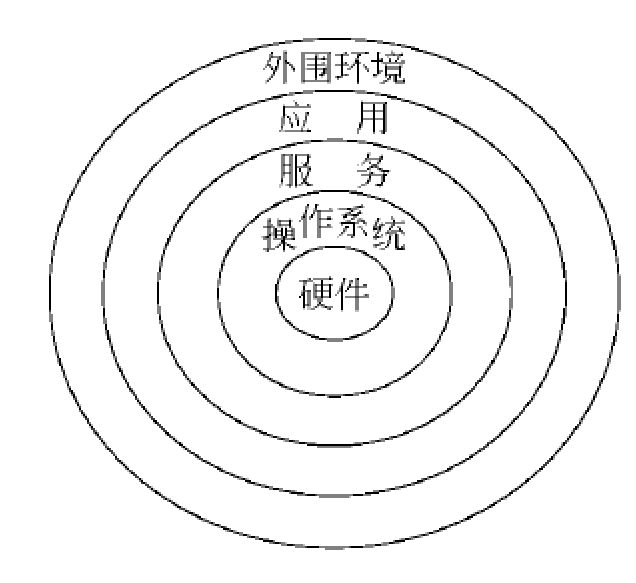


图 1-2 计算机系统的保护机制

从图 1-2 可看出，计算机系统的保护是分层次的，比如，硬件级的安全保护只涉及到硬件的保护，而涉及不到操作系统的保护，反过来说，操作系统层次的保护既能保护操作系统层次，又能保护硬件层次，然而，操作系统层次的保护也涉及不到服务层及应用层的保护。从而可以得到一个结论，硬件级的保护级别最低，而应用层的保护级别最高，也就是说，当考虑应用层的保护时，除了要考虑保护应用层以外，还要考虑服务层、操作系统层及硬件层的保护。另外，恶劣的外围环境（如电压不稳定、电磁干扰严重、机房潮湿、机房有火灾隐患等）会导致数据的损坏、各种服务不能正常工作，甚至造成硬件损坏，因此，外围环境也是计算机系统安全保护最重要的内容。

4. 集中式控制与分布式控制

计算机系统的安全策略可分为集中式控制和分布式控制两种，所谓集中式控制，就是将计算机系统所有安全问题都集中在一个被称为中央实体的控制中心进行，而分布式控制则是将系统安全分别托付给系统中的各个成员或部分成员。

集中式控制的优点是便于安全监测和管理，缺点是控制中心容易造成瓶颈。鉴此，在实际应用中通常使用的是分布式控制策略，它能有效地解决瓶颈问题，但值得注意的是，系统中不同成员之间的策略一致性问题。

1.3.3 网络安全策略

网络安全策略的目的是决定一个计算机网络组织机构如何保护企业内部网络及其信息，其策略通常包括两部分内容，总体策略和具体的规则。总体策略用于阐明安全策略的总体思想，而具体的规则用于说明什么是被允许的，什么是被禁止的。

1. 网络安全策略的等级

通常将网络安全策略划分成如下 4 个等级：

- 一切都是禁止的。
- 一切未被允许的都是禁止的。
- 一切未被禁止的都是允许的。
- 一切都是允许的。

第 1 种策略是最高保护策略，其实现方法是切断内部网络与外部网络的联系。这种策略能有效地防止内部网络遭受外来的攻击，但也把内部网络与外界隔绝，不能与外界

沟通和信息交流，在通常情况下是一种不可取的策略。

第 2 种策略是开放（允许）部分有限的资源，而对于未明确开放的资源，是禁止访问的。

第 3 种策略是禁止部分资源的访问，而对于未明确禁止的资源，是允许访问的。

第 4 种是没有安全保护的策略，其实现手段是把内部网络的全部资源完全对外开放，不加任何保护。这种策略通常也是不可取的。

2. 网络安全策略的内容

一个实用的网络安全策略包括下述内容：

- 网络管理员的安全策略。该策略要求在每台主机上使用专门的安全措施，登录用户名称，监测和记录过程等，还可以限制在网络连接中所有的主机不能运行应用程序。
- 网络用户的安全策略。该策略要求用户每隔一段时间必须改变其用户操作口令；口令必须符合安全标准形式；并定时或不定时进行检测，以了解其账户是否被别人访问过。
- 网络资源的安全策略。该策略明确规定哪些人可以访问网络资源，并规定哪些资源是可以访问的，哪些资源是禁止访问的。
- 安全检测策略。该策略主要用于当检测出安全问题时的应急处理措施。

3. 网络安全机制

网络安全机制有身份认证机制、授权机制、访问控制机制、数据加密机制、数据完整性机制、数字签名机制、报文鉴别机制、路由控制机制和业务流填充机制等。

比如“授权机制”是针对不同用户授以不同的资源访问权限的一种安全访问机制。其具体内容如下：

- 一致性。对资源的控制没有二义性，各种定义之间不能相互冲突。
- 统一性。对所有资源要求集中进行管理，安全策略必须统一。
- 审计功能。对所有授权用户都能进行审计跟踪检查。

习 题 1

1. 信息安全保密的内容是什么？
2. 信息安全内容有哪几个方面？
3. 信息安全的特点是什么？
4. 计算机的安全机制是什么？
5. 安全管理的主要功能是什么？
6. 网络安全的主要技术有哪些？
7. 网络安全策略有哪些等级？
8. 网络安全策略的内容是什么？

chapter 2

第 2 章 计算机环境安全技术

21 环境安全概述

计算机周边环境的好坏直接影响计算机及其外围设备的性能及工作，也直接涉及网络设施的安全，因此，要保护计算机及网络的安全，环境的安全是至关重要的。

计算机环境安全的内容有计算机机房场地、温度、湿度、洁净度、静电、电磁干扰、采光照明和噪声等的安全技术，本章将逐步加以介绍。

21.1 计算机机房安全

1. 计算机机房安全的内容

- 计算机机房的设备防护。火灾及防护措施、机房的防水、机房的防物理、化学、生物灾害、硬件防盗。
- 计算机机房安全供电系统。供电故障对计算机系统的影响、电源故障类型、供电系统的技术要求、计算机系统供配电技术、电源安全要点。
- 计算机机房安全接地系统。计算机机房的接地种类及其作用、计算机机房的接地系统、计算机接地装置的安装要求、接地工艺、接地电阻的测量。

2. 机房位置

计算机设备应该有足够的摆放空间，可以放置在任何一层楼，但由于一楼太潮湿、顶楼易漏雨并易遭受雷击，所以，机房不宜设在一楼和顶楼。

计算机设备应该被安放在拥有坚固结构的楼层，具有多重安全出口，并且拥有冗余电力供应。

环境安全结构策略还要考虑到的是冗余电力供应的可行性。冗余电力供应包括为设备提供电力的电力公司、不间断电源 UPS 以及一切与之相关的事项。策略必须反映出物理和经济现实，同时也要考虑到对保护业务运作的必要条件。

3. 锁和防护设施

如果要确保信息被存放在安全的房间里面，就不能不考虑门和其他防护设施。破旧

的门可能会成为物理安全程序中的脆弱之处。

防火门和防火设施可以防止或减少损失，它们可以防止外面的火势蔓延到屋内，也可以防止屋里的火冲到屋外，火可能在扩散之前就熄灭了。这些门应该是密封的，甚至可以考虑用自动关闭功能的门，这样可以更有效地防火。关于这些门的策略不仅要考虑到它们的用途，还要注意这些门不能长期保持打开状态。

4. 环境支持

环境的每一个方面都可以有对应的策略。知道如何控制静电，保持适当的湿度、温度和空气质量。

2.1.2 环境保护机制

在制订环境保护策略前，应首先对一些环境或措施有所了解，然后针对自身的情况，对相关的策略做出一个正确的定位。环境保护涉及到的主要机制和措施由空调系统、防静电和防火等方面构成，下面将作详细的介绍。

放置服务器的区域应该有足够的环境控制系统，包括温度和湿度控制以及防止静电的有效措施。

1. 温度

计算机系统内有许多元器件，不仅散热量大而且对高温、低温非常敏感。环境温度过高容易引起硬件损坏，温度太低时，有些设备工作不正常或无法正常启动。机房温度一般应控制在冬季(20±2)℃、夏季(23±2)℃，温度变化率≤5℃/h。

2. 湿度

机房内相对湿度过高会使电气部分绝缘性降低，金属锈蚀加快；而相对湿度过低会引起静电的积聚，使计算机内信息丢失、损坏芯片，使外部设备工作不正常等。机房内的相对湿度一般控制在(50±5)%。湿度控制与温度控制都应与空调联系在一起，由空调系统集中控制。机房内应安装温、湿度显示仪，随时观察、监测。

3. 粉尘

计算机及其外部设备是精密的设备，磁头的缝隙、磁头与磁盘之间读写时的间隙都非常小，一粒小小的尘埃相对这个间隙就像是一座大山，它会影响寻道的准确性，甚至划伤磁盘，严重地影响计算机系统的正常工作。因此，机房必须采取一定的除尘、防尘措施，以保证设备稳定地工作。

机房内一般应采用乙烯类材料装修，避免使用挂毯、地毯等吸尘材料。人员进出门应有隔离间，并应安装吹尘、吸尘设备，排除进入人员所带的灰尘。空调系统进风口应安装空气滤清器，并应定期清洁和更换过滤材料，以防灰尘进入。同时进风压力要大，房间要密封，使室内空气压力高于室外，这样灰尘不会进入室内。

房内的尘埃要求低于0.5nm；对于开机时机房内的噪音，在中央控制台处测量时应

小于 70dB。

4. 其他

洁净度。要求符合标准 Ashrae 52～76,空气中大于 0.5nm 的尘粒每立方米应少于 10 000 粒。

噪声。关闭主设备的条件下,在工作人员正常办公位置处测量不高于 68dB。

机房单位面积的冷负荷为 $257W/(m^2h)$。

系统控制室单位时间换气数≥23 次/h。

数据中心机房单位时间换气数≥22 次/h。

22 环境安全保护

221 空调系统

计算机房内空调系统是保证计算机系统正常运行的重要设备之一。通过空调系统使机房的温度、湿度和洁净度得到保证,从而使系统能正常工作。重要的计算机系统安放处应有单独的空调系统,计算机房的空调较一般的空调有更苛刻的要求。它应具有供风、加热、冷却、减湿和空气除尘的能力。

空调系统的送风量应取下列 3 种数据中的最大值。

- 室内总送风量的 5%。
- 按工作人员每人 $40m^3/h$。
- 维持室内正压所需风量。

主机房的空调送风系统,应设初效、中效两级空气过滤器,中效空气过滤器计数效率应大于 80%,末级过滤装置宜设在正压端或送风口。

主机房在冬季需送冷风时,可取室外新风作冷风源。

计算机机房空气调节控制装置应满足计算机系统对温度、湿度以及粉尘对正压的要求。

空调设备的选择如下:

- 空调设备的选用应符合运行可靠、经济和节能的原则。
- 空调系统应设消声装置。
- 空调系统和设备选择应根据计算机类型、机房面积、发热量及对温、湿度和空气含尘浓度的要求综合考虑。
- 空调冷冻设备宜采用带风冷冷凝器的空调机。当采用水冷机组时,对冷却水系统冬季应采取防冻措施。
- 空调和制冷设备宜选用高效、低噪声、低振动的设备。
- 空调制冷设备的制冷能力,应留有 15%～20%的余量。
- 当计算机系统需长期连续运行时,空调系统应有备用装置。

222　防静电措施

静电是由物体间的相互摩擦、接触而产生的，老式计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体表面，会有很高的电位，从而产生静电放电火花，严重时会造成火灾。还可能使大规模集成电器损坏，而这种损坏可能会在不知不觉中进行。

为避免静电的影响，最基本的措施是接地，将物体积聚的静电迅速释放到大地。为此，机房地板基体（或全部）应为金属材料并接大地，使人或设备在其上运动产生的静电随时可释放出去。机房内的专用工作台或重要的操作台应有接地平板，必要时，每人可带一个金属手环，通过导线与接地平板连接。此外，工作人员的服装和鞋最好用低阻值的材料制作，机房内避免湿度过低，在北方干燥季节应适当加湿，以免产生静电。

对于防静电直接有效的策略应为：任何人员进入防静电区域前，必须在手上或鞋上加带防静电导电环。

223　机房防火机制

计算机房的火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路会因为短路、过载、接触不良、电线老化、绝缘层破坏或静电等原因引起电打火而引起火灾。人为事故是指由于操作不慎，吸烟、乱扔烟头等，使充满易燃物质（如纸片、磁带和胶片等）的机房起火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起机房起火。

为避免火灾，应在安全策略中标明以下防火机制。

1. 分区隔离

建筑内的机房四周应设计为一个隔离带，以使外部的火灾至少可隔离 1 小时。系统中特别重要的设备，如微处理器、媒体库等，尽量与人员频繁出入的区域和堆积易燃物（如打印纸）的区域隔离。所有机房门应为防火门，外层应有金属蒙皮。计算机房内部应由阻燃材料装修。

2. 火灾报警系统

火灾的发展有 3 个阶段，发烟阶段、火焰扩散阶段和热辐射扩散阶段。火势的蔓延主要是通过热辐射扩散进行的。当火势发展到热辐射扩散阶段时，机房的温度就已达到使计算机和存储介质遭到破坏的程度了。因此，火灾报警系统的作用是在火灾初期就能检测到并及时发出警报。

火灾报警系统按传感器的不同分为烟报警和温度报警两种类型。烟报警器可在火灾开始的发烟阶段就会检测出，并发出警报，可使火灾及时被发现。而热敏式温度报警器是在火焰发生、温度升高后发出报警信号。近年来还开发出一种新型的 CO_2 探测报警器，它可以在发烟初期即可探测到火灾的发生，避免损失，且可避免人员因缺氧而死亡。

为安全起见，机房应配备多种报警系统，并保证在断电后 24 小时之内仍可发出警报。报警器为音响或灯光报警，一般安放在值班室或人员集中处，以便工作人员及时发现并向消防部门报告，组织人员疏散等。

3. 灭火设施

机房所在楼层应有消防栓和必要的灭火器材和工具，这些物品应具有明显的标记，且需定期检查。这些器材和工具包括：

- 灭火器。虽然机房建筑内要求有自动喷淋、消防供水系统和各种灭火器，但并不是任何机房火灾都要自动喷淋，有时对设备的二次污染破坏比火灾本身造成的损坏更为严重。因此，推荐使用不会造成二次污染的气体灭火器。如不具备条件，也可使用 CO_2 灭火器。
- 灭火工具及辅助设备。应急工具应有液压千斤顶、手提式锯、铁锹、挪头和撬木等。

必要时，还应准备应急自呼吸器和应急灯等。

4. 管理措施

要严格执行计算机房环境和设备维护的各项规章制度，加强对火灾隐患部位的检查。如电源线路要经常检查是否有短路处，防止出现火花引起火灾。对老化的电气线路要及时更新，要制定灭火的应急计划并对所属人员进行培训。此外，还应定期对防火设施和工作人员的掌握情况进行测试。

计算机系统实体发生重大事故时，为尽可能减少损失，应制定应急方案。建立应急方案时应考虑到对实体的各种威胁，以及每种威胁可能造成的损失等。在此基础上，制定对各种灾害事件的响应程序，规定应急措施，使损失降到最低限度。

5. 制订环境防火策略

根据上述 4 点防火机制，制订出有效的防火安全策略。通过策略，能够将火灾的隐患减到最低。针对于防火的安全策略，可以参考以下描述。

- 办公区域按建筑要求划分出明确的防火分区，并醒目地标明逃生通道。
- 由专人负责建立防火预案、报警预案、疏散预案与灭火预案。
- 必须有人员对防火报警系统进行 7×24（每周 7 天，每天 24 小时）的监视，如发现系统报警，严格执行火灾报警预案。
- 所有人员应该熟悉消防器材的放置位置，在有紧急情况时，保证能迅速启用消火栓或消防器材。
- 定期对所有人员进行防火知识培训，定期审查每个部门的防火情况。

224 电源干扰与保护装置

电源是计算机系统正常工作的重要因素。供电设备容量应有一定的储备，所提供的功率应是全部设备负载的 125%以上。计算机房设备应与其他用电设备隔离，它们应为变压器输出的单独一路而不与其他负载共享一路。在安全策略中关于电源部分的描述

应该参照以下内容来制订。

1. 电源干扰

常用的电源线干扰有6类：中断、异常状态、电压瞬变、冲击、噪声和突然失效事件。

1）中断

电源三相线中任何一相或多相因故障而停止供电为中断，长时间中断即为关闭。

2）异常状态

连续电压过载或连续低电压为异常状态。在一段时间内连续电压不足可能是因为个别负载过大而形成的降压。

3）电压瞬变

瞬变浪涌是在几个正弦波范围内，电压幅值快速增加；瞬变下跌也是在几个正弦波范围内，电压幅值快速降低。

4）冲击

冲击又称瞬变脉冲或尖峰电压，是指0.5～100μs内过高或过低的电压。尖峰一般指瞬时电压超过400V，而下垂电压指瞬时向下的窄脉冲。

5）噪声

电磁干扰是由电源线发射产生的电磁噪声干扰，射频干扰是发射频率不小于30kHz时的电磁干扰。

6）突然失效事件

突然失效事件指由核爆炸或雷击引起快速升起的电磁脉冲冲击，致使设备失效。

2. 电源保护装置

电源保护装置有金属氧化物可变电阻（MOV）、硅二极管（SAZD）、气体放电管（GDT）、滤波器、电压调整变压器（VRT）和不间断电源（UPS）等。

金属氧化物可变电阻可吸收尖峰和冲击电压，工作时间为1～5ns。SAZD和GDT可使浪涌和尖峰电压分流，从而保护电路。SAZD的工作速度快，但不能处理大的浪涌；GDT能处理大的浪涌，但工作速度较慢。滤波器通过保护电路使噪声分流，使浪涌衰减。VRT可在秒级进行异常状态保护。后备UPS可保护系统，避免断电、电源故障、供电不足和其他低电压状态的影响。连续工作的UPS可使计算机不受电源的影响，保护它们避免灾难性干扰。避雷针和浪涌滤波器可帮助抵抗强电磁脉冲。此外，安装设备时应使之远离建筑的金属结构，以避免雷击影响。

3. 紧急情况供电

重要的计算机房应配置抵抗电压不足（电源下跌）的设备，这种设备有如下几种：

1）基本UPS

基本的不间断电源UPS一般可提供15分钟以上的应急供电，这个时间可以使机房人员在断电时应急工作。供电时间的长短依赖于蓄电池的容量大小。基本的UPS包括一个整流器部件，它可使AC电源整流并不间断地使电池充电。这个电池组在断电时，可

驱动转换器向机房设备供电。

2）改进的 UPS

基本的 UPS 经改进后，增加了一个 UPS 和 AC 电源间的转换器。这样，当恢复 AC 供电时，UPS 就可自动切换到 AC 电源供电，而不必由电池继续供电。用这种方法可减少电池供电时间，延长电池寿命。

3）多级 UPS

安装多个单独的 UPS，使系统通过 UPS 可长时间连续工作。这种方式下，每个 UPS 都要求有较大容量（100KW），当一个 UPS 出现问题时，仍可继续供电，从而有效地保护系统。在特别重要的场合，应考虑这种措施。

4）应急电源

应急电源主要是通过一个发电机组提供紧急供电。在断电时启动发电机供电，可为系统提供较长时间的紧急供电，但它需要有自己的燃料支持。应急电机对最重要的设备提供支持，这包括空调、最必需的计算机、照明灯、报警系统和通信设备。

4. 电源保护策略

针对电源安全策略，可以参考以下描述。

- 电源稳定的情况下，由各部门提出重要设备，可以申请加装 UPS 电源。
- 电源不稳定情况下，包括各种不稳定因素，所有接电设备加装 UPS 电源。

225 机房防雷措施

1. 接地机制

接地指系统中各处电位均以大地为参考点，大地电位为零电位。接地可以为计算机系统的数字电路提供一个稳定的电位（0V），可以保护设备和人身的安全，同时也是避免电磁信息泄露必不可少的措施。

2. 地线种类

1）保护地

计算机系统内的所有电气设备，包括辅助设备和外壳均应接地。因为电气设备的电源线绝缘层被破坏或偶然接触时，设备的外壳可能带电，极易造成人身和设备事故，必须将外壳接地，以使外壳上积聚的电荷迅速排放到地上。

2）直流地

直流地又称逻辑地，是计算机系统的逻辑参考地，即计算机系统中数字电路的低电位参考地。数字电路只有 1 和 0 两种状态，1 代表高电位，0 代表低电位或“零”电位，其电位差只有 3～5V。随着超大规模集成电路的发展，电位差越来越小，对逻辑地的接地要求也越来越高。因为逻辑地（0V）电位的变化直接影响到数据的准确性。直流地的阻值一般要求不大于 2Ω，大型主机房的直流地的阻值要求小于 1Ω。

3）屏蔽地

为避免信息处理设备的电磁干扰，防止电磁信息泄露，重要的设备和重要的机房都要采取屏蔽措施，即用金属体来屏蔽设备和机房。这种金属体称为屏蔽机柜或屏蔽室。屏蔽体需要与大地相连，形成电流通路，为屏蔽体上的电荷提供一条低阻抗的流放通路。屏蔽效能的好坏与屏蔽体的接地密切相关，一般屏蔽地的地阻要求低于4Ω。

4）静电地

机房内人体本身、人体在机房内的运动、设备的运行等均可产生静电。人体带有的静电有时是很高的，可达1000V以上，这时人体与设备或元器件导电部分直接接触极易造成设备损坏。而设备运行中产生的静电干扰则会引起机械、读写错误等故障。为避免静电的影响，除可采取管理方面的措施，如测试人体静电、接触设备前先触摸地线、泄放电荷、保持室内一定的温度等外，还应采取防静电地板等措施以使设备运行中产生的静电随时释放。

5）雷击地

雷击具有很大的能量，雷击产生的瞬间电压可高达10万伏以上。单独建设的机房或机房所在的建筑物，必须设置专门的雷击保护地，以防止雷击产生的设备和人身事故。应将具有良好导电性能和一定机械强度的避雷针安置在建筑物的最高处，引下导线接到地网或地桩上，形成一条最短的、牢固的对地通路，即雷击地线。

3. 接地系统

计算机房的接地系统是指计算机系统本身和场地的各种接地设计和具体实施。

1）各自独立的接地系统

这种接地系统主要考虑直流地、交流地、保护地、屏蔽地和雷击地等有各自的作用，为了避免相互干扰，分别通过地网或接地桩接到大地。这种方案虽然理论上可行，但实施起来难度是很大的。理想的情况下，各地线之间要有一段距离。如果远离机房，引线太长，不仅会造成地阻太大，而且会引入干扰。而围绕机房四周埋设几个地网，因有道路、建筑和地下水管等，很难满足要求，而且建几个地网的投资也是很大的，在实际工程中很难做到。

2）交、直流分开的接地系统

这种接地系统将计算机的逻辑地和雷击地单独接地，其他接地共地。这既可使计算机工作可靠，又可减少一些地线。但这样仍需要3个单独的接地体，无论从接地体的埋设场地考虑，还是从投资和施工难度考虑，都是很难承受的。这种方案在国内一些大型计算中心的建设中曾采用过，而一般微机机房很少采用。

3）共地接地系统

共地接地系统的出发点是除雷击地外，只建一个接地体，此接地体的地阻要小，以保证释放电荷迅速排放到大地。而计算机系统的直流地、保护地和屏蔽地等在机房内单独接到各自的接地母线上，自成系统，再分别接到室外的接地体上。

这种接地的优点是减少了接地体的建设，各地之间独立，不会产生相互干扰。其缺点是直流地（逻辑地）与其他地线共用，易受其他信号干扰。目前这种接地系统广泛用于

微机机房，国外已推广应用到小型机房。

4）直流地、保护地共用地线系统

这种接地系统的直流地和保护地共用接地体，屏蔽地、交流地、雷击地单独埋设。它主要考虑的是，许多计算机系统内部已将直流地和保护地连在一起，对外只有一条引线，在这种情况下，直流地与保护地分开已无实际意义。由于直流地与交流地分开，因此使计算机系统仍具有较好的抗干扰能力。这种接地方式在国内外均有广泛应用。

4. 建筑物内共地系统

随着城市高层建筑群的不断增多，建筑物内各种设备和供电系统、通信系统的接地问题越来越突出。一方面，建筑高层化、密集化，接地设备多、要求高；另一方面高层建筑附近又不可能有足够的场地构造地线接地体。这就使建筑物内共地系统的方案呼之欲出。高层建筑目前基础施工都是先打桩，整栋建筑从下到上都有钢筋基础。由于这些钢筋基础很多，且连成一体，深入到地下漏水层，同时各楼层钢筋均与地下钢筋相连，作为地线地阻很小。正由于地阻很小，将计算机房及各种设备的地线共用建筑地，从理论上讲不会产生相互干扰，从实际应用看也是可行的。它具有投资少、占地少、阻值稳定等特点，符合城市建筑的发展趋势。

5. 接地保护策略

聘请专业人员对办公区域的接地情况作定期的检查。

226 安全监控技术

机房安全监控通常使用的是闭路电视监控系统。闭路电视监控系统是安全技术防范体系中的一个重要组成部分，是一种先进的、防范能力极强的综合系统，它可以通过遥控摄像机及其辅助设备（镜头、云台等）直接观看被监视场所的一切情况，可以将被监视场所的情况一目了然。同时，电视监控系统还可以与防盗报警系统等其他安全技术防范体系联动运行，使其防范能力更加强大。

闭路监控系统能在人们无法直接观察的场合，实时、形象、真实地反映被监视控制对象的画面，并已成为人们在现代化管理中监控的一种极为有效的观察工具。由于它具有只需一人在控制中心操作就可观察许多区域，并具有远距离区域的监控功能，被认为是保安工作之必要手段。

一个完善的安全监控系统应由下列技术组成：

1. CCTV 监控系统

根据不同的用途选择合适的系统配置，CCTV 监控系统能够满足多方面的需求。

- 室外云台。除具备室内云台所有的功能外还具有防水、防爆功能。
- 半球形彩色/黑白摄像机。吊顶式安装，外形美观，适用于各种场合。
- 彩色监视器。用于显示前端。
- 彩色摄像机的视频画面。

- 时序切换系统。在一台监视器上依次切换显示多个摄像机的图像,可以进行重点的切换画面显示,切换时间可以调整。即使摄像机数量增加,监视器也不必增加,所以该系统可以节约成本,非常经济。
- 数字分割系统。把一台监视器的画面多分割以同时显示 4~16 个摄像机的图像,只需一人就能够同时监视多个场所的现场情况。所有摄像机图像可以编程成组或切换在 1 台高清晰度监视器上同时分割显示,也可以自由切换选择按顺序单独显示或设置为 4 分割或 9 分割等显示状态。系统中的重点摄像机图像送入一台 16 画面处理器并由一台 24 小时录像机使用一盒普通 180 分钟录像带实时录像,录像可以回放,以便为管理提供证据。
- 远距离操作摄像机放大系统。全方位旋转云台彩色 32 倍变焦摄像机,通过系统控制键盘的操作可以实现摄像机图像上下左右旋转扫描,对摄像机云台转向、镜头焦距和镜头光圈等进行遥控操作,远距离捕捉现场物体的全景和放大后的细节,放大倍数可以预定。
- 数字式彩色摄像机。具有自动电子快门、自动跟踪、背光补偿及彩色还原准确等功能。

2. 闭路监控系统

闭路监控系统主要由以下几个部分组成:

- 产生图像的摄像机或成像装置。
- 图像的传输与控制设备。
- 图像的处理与显示设备。

闭路电视监控系统的技术要求主要是摄像机的清晰度、系统的传输带宽、视频信号的信噪比、电视信号的制式、摄像机达到较高画质和操作的功能以及系统各器件的环境适应度。

3. 画面处理器

画面处理器能够同时在一台显示器上显示 1~16 个画面,用一台录像机录完 1~16 个画面的信号。

4. 专业录像机

专业录像机主要由以下几个部分组成:

- 具有 24 小时的长延时录像功能、回放画面清晰的视频切换器。
- 自动视频切换器,用于视频信号的顺序切换。
- 保护罩、支架。
- 云台镜头、控制器。
- 矩阵系统键盘、矩阵系统主机。
- 解码器。

2.3 机房管理制度及人员管理

2.3.1 机房管理制度

保持机房内的清洁卫生，上机人员不得在机房内吃零食、随地吐痰、大声喧哗、乱扔杂物，机房内严禁吸烟。

为防止病毒感染，破坏其内部文件及数据，严禁任何人私自带软盘、光盘、U 盘进入机房操作。

操作人员要严格遵守计算机操作规程，不得在键盘、鼠标上胡乱摭按，以免冲乱系统，丢失数据，损坏机器。

操作人员未经允许不得随意将盘片或软件进行复制、备份。不得将机房内的资料随意带出机房。

在对数据库作任何维护之前，输入的重要数据文件应先备份再维护。定期进行备份处理，防止意外丢失。所有数据每天都必须做好备份工作，妥善保存备份数据，定期作系统和数据备份。

在使用软件时，必须使用通过正当渠道购买或得到的软件，在使用前必须先进行病毒检测。机房管理人员应对计算机房的系统定期进行病毒检测。

涉及国家机密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔断。涉及秘密的统计资料和信息不得在与国际互联网相连的计算机信息系统中存储、处理和传递。

计算机设备和机房应保持其工作环境整洁，保持其所必须的湿度。

计算机房应列为单位要害和重点防火部门，按照规定配备足够数量的消防器材，机房工作人员要熟悉机房消防器材的存放位置及使用方法，并定期检查更换。

严禁带电拔、插各种接口插头，不得私自拆卸机器、机内主要器件应编号存档。

2.3.2 机房人员管理

加强对机房管理人员尤其是网络管理员的素质教育和职业道德教育，定期对机房管理人员进行安全及保密教育。

机房管理人员及机房计算机操作人员要坚定防范计算机病毒的思想，杜绝计算机病毒的输入、扩散和传播行为。

严禁管理人员越权操作，对重要的计算机信息处理系统应分级加设系统口令，以防机密信息的泄露。

调离人员必须移交全部技术资料和有关文档，删除自己的文件、账号，由系统管理员修改有关的口令。

习 题 2

1. 计算机环境安全包括哪些内容?
2. 环境保护机制包括哪些内容?
3. 防静电措施的内容是什么?
4. 防火安全策略有哪些内容?
5. 常用的电源线干扰有哪几种?

第3章 chapter 3

计算机系统安全与数据备份技术

当今，人们依赖于计算机系统的程度越来越大，应用面也随之越来越广。可是计算机并不安全，它潜伏着严重的不安全性、脆弱性和危险性。造成不安全的因素很多，有计算机系统本身的不可靠性；环境干扰以及自然灾害等因素引起的；也有工作失误，操作不当造成的；而人为故意的未授权窃取、破坏，敌对性活动危害更大。加上近年来计算机病毒严重地侵入计算机系统，不安全性就显得更为突出。在计算机系统中，以微型计算机安全的缺陷为最大，也最易受病毒的感染。有人曾预言，今后在现代化战争中可以利用传输病毒来破坏对方的军事指挥通信系统，使其处于瘫痪状态。因而对计算机安全问题决不能掉以轻心。

何为"计算机安全"？国际标准化委员会对计算机安全的定义提出建议，即"为数据处理系统建立和采取的技术的和管理的安全保护，保护计算机硬件、软件，数据不因偶然的或恶意的原因而遭破坏、更改、显露"。计算机安全包括实体安全、软件安全、数据安全和运行安全。从内容来看，包括计算机安全技术、计算机安全管理、计算机安全评价、计算机犯罪与侦查、计算机安全法律以及计算机安全理论与政策等内容。

另一方面，计算机网络是现代人类生活最重要的组成部分，而网络安全最根本的任务是计算机系统的安全，只有当计算机系统的安全得到了有效的保证，才能有效地保证数据的安全和网络的安全。

本章着重介绍的就是计算机系统的安全保护技术，包括计算机硬件安全技术、计算机软件的安全技术以及计算机口令安全技术。

3.1 计算机硬件安全技术

计算机硬件及其运行环境是网络系统运行的最基本因素，其安全程度对网络的安全有着重要的影响。由于自然灾害、设备自然损坏和环境干扰等自然因素以及人为有意或无意的破坏与窃取等原因，计算机设备的安全就会受到很大的威胁。本节讨论的是网络系统中硬件设备及其运行环境，以及面临的各种安全威胁和防护策略。

3.1.1 硬件安全内容及硬件保护机制

1. 计算机硬件安全内容

- 计算机(含服务器及终端计算机)。
- 存储设备(硬盘、光盘、磁带等)。
- 网络通信线缆(光缆、双绞线、同轴电缆等)。
- 网络连接设备(交换机、路由器、防火墙、调制解调器等)。
- 灾难。防雷、电、雨、水、火。
- 环境。静电、烟、灰尘、温度、湿度。
- 破坏。人、盗、鼠、病毒。
- 供电。UPS。
- 主机。双机热备份、异地备份(冗余备份)。
- 存储。磁盘镜像、磁盘阵列、光盘塔、磁带。

2. 硬件保护机制

硬件是组成计算机的基础。硬件保护包括两个方面,一方面指在计算机硬件(包括CPU、内存、缓存、输入/输出通道和外围设备等)上采取的安全防护措施,另一方面是指通过增加硬件设备而达到安全保密的措施。随着计算机技术的发展,超大规模集成电路的广泛应用使计算机的功能越来越完善,更新换代也越来越快。由于硬件安全防护措施的开销大,且不易随着设备的更新换代而改变,因此,许多安全防护功能是由软件来实现的。软件保护措施灵活、易实现、易改变,但它占用资源多、系统开销大,并且运行起来会降低计算机的功能。此外,完全依赖软件的一些保密手段(比如磁盘加密程序)易被软件破译,增加硬件保护才能保证安全可靠。由于这种原因,硬件防护措施仍是计算机安全防护技术中不可缺少的一部分。特别是对于重要的系统,需将硬件防护同系统软件的支持相结合,以确保安全。例如,虚拟存储器保护是一种硬件防护措施,但是其动态地址转换功能需要有一套虚拟存储空间的表格结构,这就需要操作系统的支持。

3.1.2 计算机主设备安全

1. 计算机加锁

计算机加锁是将计算机的重要控制电路的通断用锁来控制。早期的加锁部分包括键盘、内存和硬盘等。由于机械锁常造成电路损坏并诱发故障,现代计算机多采用数字电路锁,将开锁的密码保存在电路中,只有知道密码才能使用设备,如CMOS口令替代了以往的键盘锁。

2. 信息保护卡

防复制卡,插座式的数据变换硬件(如安装在并行口上的加密狗等)可成为软件运行

的必要条件。由于硬件的不可复制性,限制了软件的非法复制和流传。硬盘保护卡是一种能够保护硬盘数据的硬件卡,有两种主要类型,备份型保护卡和标记型保护卡。备份型保护卡将硬盘分成两部分,一部分备份原始数据,另一部分供用户使用,表面上看硬盘损失了一部分,但安全性比较高。标记型保护卡不损失硬盘空间,但安全性不如备份型保护卡。

3.1.3 计算机外部辅助设备安全

1. 打印机安全

打印机属于精密机电设备,使用时一定要遵守操作规则,出现故障时一定要先切断电源,数据线不要带电插拔。打印敏感信息产生的废稿一定要及时销毁,对于重要数据部门的打印机,要有使用记录。

2. 磁盘阵列和磁带机安全

对于磁盘阵列和磁带机安全要注意防磁、防尘、防潮、防冲击,避免因物理上的损坏而使数据丢失。例如灰尘容易在磁头上聚集,会降低磁头的灵敏度,甚至划伤磁盘或磁带,从而会造成数据的丢失,严重时会导致硬盘或磁带的损失,或者划伤硬盘片,使硬盘报废,造成重大损失。

3. 终端安全

为了防止他人非法使用计算机终端,可以在终端上加锁,终端与主机之间的通信线路不宜过长,以免被窃听。显示敏感信息的显示器要远离公众,要防止远程偷窥;采用射频通信的显示终端还要防电磁辐射泄漏。

3.2 计算机软件安全技术

3.2.1 软件安全保护的对象及软件安全内容

1. 软件安全保护的对象

- 操作系统(DOS、Windows、Windows NT、UNIX 等)。
- 网络软件(E-mail、IE、Telnet、FTP 等)。
- 工具软件(诊断软件、防病毒软件、端口扫描软件等)。
- 应用程序(会计核算软件、库存管理软件等)。

2. 软件安全内容

- 软件的授权与访问。
- 软件漏洞及补丁。

- 软件崩溃与软件恢复。
- 软件版权保护。
- 黑客攻击。
- 病毒侵袭。
- 现场保护技术。
- 用户登记簿。
- 软件管理。

3.2.2 软件共享安全技术

在早期的计算机网络系统中，应用软件是采用面向主机的集中式管理方式，即将所有用户应用软件和数据都集中存放在一台网络主机上，各个用户终端则根据各自的使用权限来访问相应的应用软件和数据。这种管理方式最大的优点在于软件和数据能保持高度的一致性，并给软件的维护和管理带来极大的方便。但这种管理方式有其致命的弱点，一是主机负担过重，尤其是在大型网络中随着用户终端数量的增加和应用软件数量的增加，系统的效率便随之下降。其二，一旦网络主机故障或网络主机不开机，则用户终端无法使用相应的应用软件。其三，集中存放在一起的数据的安全性得不到保证。分布式应用软件管理模式就是解决上述问题的有效方法，分布式管理模式就是将应用软件分别存放在用户终端上，比如有 10 台计算机上要用 100 个应用程序，就要求这 10 台计算机都要装上这 100 个应用程序。分布式管理方式的弱点，一是软件的管理和维护不方便，二是应用软件经多次维护和修改后，很难保持其软件的一致性。如何解决软件分布和软件一致性，是对网络管理的一项严峻的挑战。

3.2.3 软件分布管理模式

前面介绍的软件集中式管理方式带来了管理和维护的方便，一致性得到保证但软件的系统效率不高，软件的分布式管理方式使得软件的使用效率提高，但软件的一致性难以得到保证。解决这一问题可以采用折中的方法，即采用多个分布式文件服务器管理模式，在一个大型网络系统中配置多台文件服务器，每一台文件服务器为相关的一部分应用软件服务。可以这样理解，将所有的应用软件进行分类，将不同类别的应用软件分别存放在不同的文件服务器上，这样既解决了软件的一致性和管理维护的方便性，又能充分发挥网络系统的效率。

3.3 计算机系统的安全级别

为了对计算机系统进行安全评估，按处理信息的等级和应用的相应措施，可将计算机安全分为 A、B、C、D 4 个等次 8 个级别（如表 3-1 所示），最低级为 D 级，最高级为 A 级。从表 3-1 中可以看出，随着安全等级的提高，系统的可信度随之增加，风险也逐渐减少。

表 3-1 计算机安全等级划分表

等次	级别	名称	主要特征
A	超 A1		最理想的安全保护级别
	A1	验证设计	形式化的最高级描述和验证,形式化的隐藏通道分析,非形式化的代码对应证明
B	B3	安全区域	存取监控,高抗渗透能力
	B2	结构化保护	形式化模型/隐通道约束,面向安全的体系结构,较好的抗渗透能力
	B1	标识的安全保护	强制安全控制、安全标识
C	C2	可控制的存取控制	单独的可查性、广泛的审计跟踪能力
	C1	自主安全保护	自主存取控制
D	D	低级保护	安全保护能力最弱

3.3.1 非保护级

非保护级是最低一级,即是“低级保护”级,在表 3-1 中为 D 等 D 级别,其安全保护能力最弱。这一级别是专为经过安全评估,但满足不了高水平评估系统设计的,也可以说,属于非保护级的系统是一些不符合安全要求的系统。因此,可以认为非保护级的系统是不能在多用户环境下处理敏感信息的。

3.3.2 自主保护级

在表 3-1 中,C 等为自主保护级,具有一定的安全保护能力,其采用的主要措施有自主访问控制和审计跟踪两种,其选用范围是具有一定等级的多用户环境。自主保护级能为各级提供无条件的安全保护,并通过审计追踪,对主体及其产生的动作负责。

自主保护等级分为 C1 和 C2 两个级别,即自主安全保护级别和可控制的安全保护级别。

1. 自主安全保护级(C1 级)

自主安全保护级别的系统能提供用户与数据相隔离的能力,以符合自主保护的目的。其主要技术是系统包含了许多可信控制方式,能在个体基础上实施存取限制,即允许用户保护自己的隐私和私密性信息,使其免遭非法用户浏览和破坏。

C1 级是通过系统提供用户与数据相隔离的功能,满足 TCB(Trusted Computing Base,可信计算基础)自动安全的要求。TCB 是操作系统中用于实现安全策略的一个集合体,包含软件、固件和硬件的集合,该集合体根据安全策略来处理主体对客体的访问,并满足以下特征,TCB 实施主体对客体的安全访问、TCB 是防篡改的、TCB 的结构易于分析和测试。这里所提及的“可信计算基础”是一个安全计算机系统的参考校验机制,包

含了所有负责实施安全的策略以及对保护系统所依赖的客体实施隔离操作的系统单元，它是计算机系统内保护装置的总体，包括硬件、固体、软件和负责执行安全策略的组合体。TCB 建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。换句话说，就是所有与系统安全有关的功能均包含在 TCB 中。

在这一级中，TCB 应在客体之间定义和进行访问控制。它采用的安全机理（安全机理有个人控制、组控制、公共控制和访问控制）应允许客体拥有者指定和控制客体是由自己使用，还是由用户组或公共使用。满足该级别的系统在进行任何访问操作之前，必须由 TCB 确认用户的身份（可采用口令等方式进行用户的身份认证），并保护数据，以免未经授权的用户对确认的数据进行非法的访问和修改。通过用户拥有者的自主定义和控制，可以防止自己的数据被别的用户有意或无意地读出、篡改、干涉和破坏，同时能提供软件和硬件的特性，定期检查其运行的正确性。系统的完整性要求硬件和软件能同时保证 TCB 连续的有效操作特性。

2. 可控制的安全保护级（C2 级）

C2 级系统比 C1 级更具有自主访问控制的能力。通过注册过程，同与安全有关的事件和资源隔离，使得用户的操作具有可查性。在安全方面，除具备 C1 级的所有功能外，还提供授权服务功能，并可提供控制，以防止存取权力的扩散。具体来说，应确定哪些用户可以访问哪些客体，而未授权用户是不能访问已分配访问权限的客体的。另一方面，C2 级还提供了客体的再用功能，即对于一个还未使用的存储客体，TCB 应该能够保证客体不包含未授权主体的数据。

此外，C2 级还能提供唯一的识别自动数据处理系统中各个用户的能力；提供将这种身份与该客体用户发生的所有审计动作相联系的能力。C2 级系统能与该识别符合，可审计所有主体进行的各种活动；能够对可信计算机 TCB 进行建立和维护，对客体存取的审计进行跟踪，并保护审计信息，防止被修改、毁坏或未经授权访问。

早期的 DEC 公司的 VAX/VMS 操作系统和 Novell 公司的 Netware 操作系统，以及现代的 Microsoft 公司的 Windows NT 操作系统都是提供 C2 级保护的系统。

3.3.3 强制安全保护级

B 等为强制保护级，这一等级比 C 等级的安全功能有很大的增强。它要求对客体实施强制访问控制，并要求客体必须带有敏感标志，可信计算机利用它去施加强制访问控制。

强制安全保护分为 B1 级（标记安全保护级）、B2 级（结构化保护级）和 B3 级（安全区域级）3 个级别。

1. 标记安全保护级（B1 级）

B1 级除了具有 C1 级和 C2 级的自主访问控制功能外，还增加了强制存取控制，组织统一干预每个用户的存取权限。可以说，B1 级具有 C2 级的全部安全特性和功能，并增加了数据标记，以标记的形式决定已命名主体对该客体的存取控制。

2. 结构化保护级(B2 级)

从 B2 级开始,按“最小特权”原则进行安全保护控制,即取消“权力无限大”的“特权用户”。任何一个人都不能享有操纵和管理计算机的全部权力。本级的主要功能是将系统管理员和系统操作员的职能与权限相分离,系统管理员负责对系统的配置和可信设施进行强有力的控制和管理,系统操作员则是操纵计算机的正常运行。本级将强制存取控制扩展到计算机的全部主体和全部客体,并且要发现和消除能造成信息泄露的隐蔽存储信道。为此,本级计算机安全级的结构,将被自行划分为与安全保护有关的关键部分和非关键部分。

3. 安全区域级(B3)

B3 级在计算机安全方面已达到目前能达到的最完备的级别。按照最小特权的原则,B3 级增加了安全管理员,将系统管理员、系统操作员和系统安全管理员的职能相隔离,使其各司其职,将人为因素对计算机安全的威胁减至最小。

B3 级要求在计算机安全级的结构中,没有为实现安全策略所不必要的代码。它的所有部分都是与保护有关的关键部件,并且它是用系统工程方法实现的,其结构复杂性最小,易于分析和测试。本级在审计功能方面不但能详细记录所有安全事件,而且能自动发出安全报警信号。

3.3.4 验证安全保护级

计算机系统的安全保护级别最高的等级是 A 等的验证安全保护级。其最显著的特点是从形式设计规范说明和验证技术进行分析,并高度地保证正确地实现 TCB。其实现技术是使用形式化验证方法,以保护系统的自主访问和强制访问,控制机理能有效地使用该系统存储和处理秘密信息或其他敏感信息。

验证保护级分为验证设计级(A1 级)和超 A1 级两个级别。

1. 验证设计级(A1 级)

A1 级的安全功能与 B3 级基本相同,但最明显的不同是本级必须对相同的设计,运用数学形式化证明方法加以验证,以证明安全功能的正确性。

在这里,无论使用何种特殊规格语言或验证系统,对该级的设计验证必须遵循以下 5 条原则:

- 必须能对安全策略的形式化模型进行清晰地验证和文件化,包括要求用数学方法证明模型与公理的一致性,模型对安全策略支持的有效性。
- 形式化顶层规格说明必须提出包括 TCB 完成功能的抽象定义和用于支持隔离执行区域的硬件或固件机制的抽象定义。如有验证工具,应使用形式化技术证明 TCB 的形式化顶层规格说明和模型的一致性,否则可采用非形式化技术。
- 必须能用非形式化技术证明 TCB 的工具(如硬件、固件和软件)与形式化顶层规

格说明的一致性。还能用非形式化技术证明形式化顶层规格说明的各要素对应于 TCB 的各单位。形式化顶层规格说明必须能表示符合安全策略要求的统一保护机制,而且 TCB 各单元的映射正是保护机制的要素。

- 必须使用形式化分析技术去标识和分析隐蔽信道,非形式化技术可用于标识隐蔽定时信道,在系统中,必须对被标识的隐蔽信道的连续存在加以说明。
- 为了配合 A1 级所要求的 TCB 扩展设计和开发分析,需要更严格的配置管理,并建立把该级安全地分配到现场的过程。

2. 超 A1 级

超 A1 级是最安全、最理想的安全保护级别。

超 A1 级系统涉及的范围包括系统体系结构、安全测试、形式化规约与验证和可信设计环境等。

1) 系统体系结构

必须给出一种形式化的(或非形式化的)证明,以表明在 TCB 中对基准监控器的自身保护和完备性确实已经实现。

2) 安全测试

对此虽然已经超出了现代技术,然而人们还是期望在形式化顶层规格说明或形式化底层规格说明中自动实现某些测试实例的生成。

3) 形式化规格说明和验证

必须在可行的场合使用形式化验证方法,使对 TCB 的验证向下扩展到源代码级。已经证明对操作系统有关安全部分源代码的形式化验证是一项困难的任务。有两项重要的考虑,一是选择一种能完全形式化表达语义的高级语言;二是对于底层规格说明经过一系列的步骤,仔细地将抽象的形式化设计映射成可实现的公式形式。经验表明,只有当最底层规格说明与实际代码一致时,才能成功地实现代码证明。

4) 可信设计环境

只有可信赖的人使用可信的设施,才能设计合格的 TCB。

3.4 口令安全技术

3.4.1 口令安全策略

密码已经成为现代人类生活的一部分,几乎所有计算机及网络系统、通信系统都需要密码,以拥有易于实现的第一级别的访问安全性。各级 IT 专业人员和用户所面临的问题是,如何使用这些密码以及如何才能不遗忘它们。密码和密码方案必须难以破解而易于牢记。因为密码如果难以记忆和理解就会造成很大的不方便,所以人们往往只花很少的精力创建简单的易于记忆的密码,因此,就会危及到自己和他人的信息安全。通过了解密码的构成与创建密码的方案,技术人员就可以为企业制订出完善的密码管理方案。为确保网络安全运行,保护所拥有的权益不受侵害,可以制订如下管理策略。

1. 网络服务器密码口令的管理

- 服务器的口令和密码，由部门负责人和系统管理员商议确定，必须两人同时在场设定。
- 服务器的口令须部门负责人在场时要由系统管理员记录封存。
- 密码或口令要定期更换，更换后网络系统管理员要立即销毁原记录，将新密码和口令封存。
- 如发现密码及口令有泄密迹象，系统管理员要立刻报告部门负责人，有关部门负责人报告安全部门，同时要尽量保护好现场并记录。需接到上一级主管部门批示后再更换密码和口令。

2. 用户密码及口令的管理

- 对于要求设定密码和口令的用户，由用户方指定负责人与系统管理员商定密码及口令，由系统管理员登记并请用户负责人确认（签字或电话通知），之后系统管理员设定密码及口令，并保存用户档案。
- 当用户由于责任人更换或忘记密码、口令时要求查询密码、口令或要求更换密码及口令的情况下，需向网络服务管理部门提交申请单，由部门负责人或系统管理员核实后，对用户档案做更新记载。

3. 密码技术基础

密码是系统和个人信息安全的第一道防线。这个系统的规模可以是任何大小，从一台计算机到一个住宅报警系统到由数百或数千台计算机组成的企业网络；信息可以是任意类型的，从社会保险号码到私人信件，再到机密文档。通过与用户名的结合，密码向用户提供了一套访问这些系统的凭证。用户名通常是某种形式的“账号”，创建它是为了让用户将它和密码一起使用。

许多用户认为用其办公桌抽屉来隐藏密码是足够安全的，但事实证明恰恰是最不安全的。另一个经常用来存储密码的地方是掌上计算机个人数字助理（Personal Digital Assistant，PDA）。如果 PDA 从不会丢失或被盗这种方法将很好，实际上存在着用于 PDA 的安全性解决方案，如 PDA Secure，它是一种通过加密对用户的 PDA 添加保护的程序。但是应该避免在用户的 PDA 或像办公桌抽屉这样显眼的位置存储密码。

4. 弱密码

弱密码就是易于被破解的密码，也是在密码设置中不可取的密码。弱密码有下列特征。

- 系统默认密码（空密码、内置账户）。
- 密码与个人信息相关（如姓名、生日等）。
- 密码为字典中的词语。
- 过短密码（密码长度小于或等于 6 位）。

- 永久密码。

5. 低效密码

设计良好密码的第一步是研究在创建密码时不应该做什么。首先，避免使用字典字。任何来自字典的字都容易受到攻击，并且，如果不经常更改它，它最终将被破解。用字典字创建密码的主要问题在于，任何密码破解工具最终都能够使用字典攻击猜到它。此外，别指望将字典字反过来写，或者在字典字后面添加简单的数字值。这些密码破解工具同样也会尝试这些组合。以下是低效密码的一些示例。

Cracker

cracker1

Rekcare

在创建密码时还要避免其他几个问题。

绝不要将个人信息用作密码的基础。举例来说，如果用户的生日是8月16日，则不要将所有的密码设置成0816、1608或者816。任何了解用户的人都可以轻易猜出这些密码。不要将与自己熟悉的人或经常提起的人的名字用于密码，也不要以这些名字作为密码建立的基础。还要避免使用身边的物品名称作为密码或密码的基础，这会使别人根据用户的物品猜出用户的密码。

不要将密码文件保存在本地机器或共享的网络上。这仅是通过文件级别访问来进行保护的，而且机器本身可能被泄漏。如果有人对某个文件夹重新设置许可权，并且错误地设置了许可权，那么该文件夹内的子文件夹的许可权也被重新设置，这会引起泄漏该网络上的所有密码。

6. 如何创建有效的密码

以下是创建有效密码的一些通用规则。

保存密码的唯一安全的地方是用户的脑袋或上锁的保险箱，只有用户自己知道这个保险箱的开箱密码组合。

有效密码必须相当长，但又不能长到让用户无法记住它们的程度。

以合理的方式使用特殊字符、大写字母和数字。如果系统有“区分大小写”的功能，则将大写字母和小写字母结合起来使用可以提供一些保护。这样，可以使用密码 Hey You，它与 heyyou 不同。加入大写字母后就添加了一层复杂性，使密码更难破解。

7. 口令加密技术

为了防止口令受到意外的攻击，比较安全的策略是把口令表(保存口令的数据文件)加密。加密后攻击者不能读取和使用口令。两种常用的加密方法是采用传统的密钥加密方法和单向函数加密方法。

在传统的加密方法中，是把整个口令加密或只把口令的某一列加密。当接收用户的口令时，把存储的口令解密，然后比较两个口令。

单向函数加密法是一种比较安全的策略。它采用一个加密函数，使加密变得相对容

易,但解密却很困难。例如,单向函数 X 简易计算,而它的反函数则不容易计算。口令表中的口令以加密的形式存储,当用户输入口令时,口令也被加密。然后比较加密后的口令。如果两者相同,那么证实该用户为合法用户。并允许使用其权限范围内的任何资源,但不允许两个不同的口令加密成相同的密文。

3.4.2 开机口令

目前 PC 是世界上使用最多的计算机,PC 上运行的操作系统多为 MSDOS 或 Windows 2000/XP/2003 等,而 Windows 2000/XP/2003 系统简单易学,且具有友好的界面、丰富的应用软件,成为了个人用户的首选。然而,由于 Windows 2000/XP/2003 本身存在许多安全性方面的问题,是十分容易被攻击的。

而在另一方面,因为 Windows 2000/XP/2003 的流行,许多黑客工具在设计时就考虑了 Windows 2000/XP/2003 的兼容性,许多黑客也利用它来攻击网络系统。因此,对于个人计算机系统,用启动开机口令的开机验证机制防止非法用户使用计算机,是非常必要的。开机口令的开机验证机制是由计算机的 BIOS(Base Input/Output System)程序来管理的(即在 CMOS 下进行设置)。下面将介绍这方面的内容。

3.4.3 CMOS 口令

1. 密码破解方法

在日常的工作中,常碰到一些用户由于遗忘了 CMOS 口令或无意中设置了 CMOS 口令,致使计算机无法启动操作系统或无法进行 CMOS 参数设置,很多用户对此束手无策,只能送计算机公司修理,耽误了很多时间。

其实,根据 CMOS 口令的设置情况,可以有很多方法来破解,其原则是,如果设置了 CMOS 开机口令,必须采用硬件或 CMOS 万能密码法破解;如果仅设置了 BIOS 设置口令,破解这种口令简直易如反掌。下面给出破解 CMOS 口令的几种方法。注意,这些方法当然也有可能会被黑客们利用,因此亦应针对这些破解方法,做好自己计算机的 CMOS 口令保护。

2. 硬件法破解 CMOS 口令

如果将 BIOS 设置中的 SEURITY OPTION(密码属性)设为 ALWAYS/SETUP 或 SYSTEM,则更是不幸中的不幸,因为此时既无法进入 CMOS 设置程序更改口令,也无法启动操作系统,这种情况只能采取在硬件上进行 CMOS 掉电处理和使用万能密码这两类方法解决。

首先需要提及的是,硬件破解的各种方法均需在计算机关机的状态下进行(最好将电源线拔掉),先清除人身上的静电,再打开计算机机箱,否则可能导致计算机硬件的损坏。

1) 跳线/开关放电破解法

计算机主板上一般都有 CMOS CLEAR(CMOS 清除)跳线,可参照计算机主板说明

书或主板上印制的跳线说明，用导体在该位置上跳接一下(即将其短路)，CMOS 口令就被清除，开机后即能进入 CMOS 设置，可重新设置开机口令。之后，关机并拔掉电源线，再次将 CMOS 的 CLEAR 跳线位置开路。

2）导线划芯片放电破解法

硬件破解 CMOS 口令的本质是让 CMOS RAM 芯片掉电，使其中保存的设置丢失，从而达到清除 CMOS 口令的目的，抓住了这一点，在解决此类问题时，可先将 CMOS 电池卸下，然后用一根导线，将其一端接到 CMOS 电池插座的地线端，用另一端在 CMOS RAM 片的两排脚上轻轻地一扫而过(如不能确认哪块是 CMOS 芯片，则可多扫几块芯片，扫时注意别损伤了芯片引脚)，CMOS 密码便会被清除。此方法适用于计算机主板上没有设计 CMOS CLEAR 跳线的情况。

3）卸电池等待法

这是一种麻烦和消极的方法。CMOS 是靠主板上的一块电池及相应的附属电路来提供电源以保持设置信息的，因此，如果将 CMOS 电池取下，再将电池接口的正负极(注意不是电池的正负极)短路，然后等待一段时间后，CMOS 供电电路中残存的电能将会消耗完，CMOS 口令就会被清除了。

如果 CMOS 电池是焊接在主板上的，则需先焊下来再试用上述的第 2、3 种方法。所以只有在确认主板上确实没有设计 CMOS CLEAR 跳线的情况下，才可采用后两种方法。

3. 用 CMOS 万能密码破解开机口令

如果计算机机箱加锁(比如众多的进口原装计算机)或因为其他原因无法打开机箱，自然也就无法进行上述的硬件破解法，是否还有其他方法能破解 CMOS 开机口令呢？答案是肯定的，下面介绍一种不用拆机箱的软方法"万能密码法"。

破解原理：在 BIOS 的密码中也有像 WPS 那样的万能密码，但不同的 BIOS 厂家有不同的密码。

1）用 CMOSPWD 获取 CMOS 万能密码

计算机 BIOS 的版本很多，不同版本的万能密码也不一样，想用几个密码"通行"于所有版本的 BIOS 显然是不可能的。那么如何获得更多的万能密码呢？在 Internet 网上有一个运行在 DOS 环境下的 CMOSPWD. EXE 软件可以做到这一点。

CMOSPWD 工具可以获取多种 BIOS 类型的 CMOS 码。因此，当忘记了计算机的 CMOS 密码时，可找一台相同的计算机，给其设置上开机口令，然后运行 CMOSPWD 找到"万能钥匙"，再用到自己的计算机上即可。

2）用 UNAWARD 获取 AWARD BIOS 万能密码

UNAWARD. EXE 可以帮助用户轻松地获得 Award BIOS 的万能密码，还可以用该软件 DISABLE(禁用)这些万能密码，甚至删除这些密码。

通常同型号主机的 AWARD BIOS 万能密码是一致的。因此当忘记了 AWARD BIOS 密码时，不用着急，试着在身边找找或打电话问问朋友们的主板型号、厂商是否与自己的这台主机主板相同，假如有的话，用 UNAWARD. EXE 将那台计算机上的密码获

取后再传回来，一切就大功告成了。

注意，若需 BIOS 的万能密码，必须先在超级用户密码（SUPERVISOR PASSWORD）中设置密码，如没有超级用户密码选项，则必须在用户密码（USER PASSWORD）中设置密码，否则该软件不能用作 BIOS 的万能密码。

3）使用通用 CMOS 密码

目前大部分主板使用 AWARD 公司的 BIOS 程序，部分主板使用 AMI 公司的 BIOS 程序，某些厂家在生产主板时为自己的 BIOS 预留了通用 CMOS 密码，以解一时之需。其中 AWARD BIOS 只有 4.51 版以前的才有通用密码。通用密码如下：

AWARD BIOS：wantgirl Syxz dirid ebb h996 wnatgirl Award

AMI BIOS：Sysg

4. 其他破解方法

如果在计算机的 BIOS SETUP 程序中设置了 CMOS 口令，但在 PASSWORD OPTION（密码选项）中选择为 SETUP 时，不必打开机箱，只要简单地利用上面介绍的万能密码程序在当前计算机上运行一下，即可轻松和准确地获得这台计算机的 CMOS 万能密码，然后用此万能密码即可进入 BIOS SETUP 程序中更改各种 CMOS 参数了。

1）用 DEBUG 破解 SETUP 设置口令

在计算机的 BIOS SETUP 程序中设置了口令，但在 PASSWORD OPTION 中选择为 SETUP 时，利用 DOS 中的 DEBUG 程序清除 CMOS 口令。

当计算机接通电源时，首先执行的是 BIOS 加电自检程序，对整个系统进行全面的检测，其中也要对 CMOS RAM 中的配置信息有关单元作累加和测试，并与原来的存储结果进行比较，当两者相吻合时，则 CMOS RAM 中的配置有效，程序继续进行其他测试，当发现累加和与原值不相等时，则要求重新配置，并能自动地按实际情况进行最小配置的设定，此时原来的 CMOS 口令也会被自动消除。

利用这一点，只要往 CMOS RAM 中的 80 口 10H～2DH（配置信息存放单元）中的任一单元写入一个数，即可清除 CMOS SETUP 口令。具体操作如下：

在 DOS 屏幕下，先运行 DEBUG 程序，输入：

```
C> debug   <回车>
- o 7010   <回车>
- o 71     <回车>
- q        <回车>
```

然后重新启动系统，密码即被清除，系统将要求重新配置 CMOS 参数，这样便可以重新进入 BIOS SETUP 接口去设计系统配置。

2）输入代码破解 SETUP 设置口令

使用本方法生成的可执行文件能够清除 CMOS 密码。本方法的最大特点是不需使用任何工具软件，而只需简单地使用 DOS 内部的 COPY 命令，从键盘上输入所需代码，并生成所需的破解程序。

```
C: > copy con cmos.com
179,55,136,216,230,112,176,32,230,113,254,195,128,251,64,117,241,195 ^Z(F6)
<回车>
```

注意,输入上述数字时必须用键盘上的 Alt 键加小键盘上的数字键来输入,其中的逗号表示输入到该处时松一下双手再继续输入,而非真的输入逗号;"^z"代表按 Ctrl+Z 组合键或按 F6 键,结束文件输入,最后按 Enter 键在当前目录下生成可执行文件。

在 DOS 下运行生成可执行文件 cmos. com,再重新冷启动计算机,会发现原来的 CMOS 设置口令已经被清除了。同样需注意的是,该方法在某些计算机上可能会不起作用。

注意,对于不熟悉计算机系统内核结构和不熟悉 DEBUG 用法的用户,最好不要使用上述两种方法。

5. 防范 CMOS 密码的破解

通过对几种常见 CMOS 密码破解方法的介绍,可以了解到要破解 CMOS 密码的前提条件。采用硬件破解法必须能够打开机箱,因此防止硬件破解法的主要措施是给主机机箱加上物理锁。

对于采用万能密码,目前没有好的防范措施,如果非法用户持有万能密码,这开机密码的安全保护措施就失去了效用,只能靠其他的安全措施防范,如通过操作系统的安全机制。另外市场上有些硬盘保护卡和防毒卡也有开机保护机制和密码机制,也能起到 CMOS 密码的功能,且破解的可能性要比 CMOS 密码机制更难些。

要防范采用工具软件破解 CMOS 密码,最主要是不能让非法用户在被保护的计算机物理性地执行工具软件,可采用如下措施。

- 屏蔽计算机的软驱和光驱,使之不能从软驱和光驱引导操作系统。
- 使用者不能在计算机处于交互状态(即可执行用户命令的状态)时离开计算机,如若离开计算机,应该关机、锁定键盘或使计算机处于安全保护状态(例如 Windows 2000/XP 系统的带密码屏幕保护状态)。
- 有条件的用户可以给计算机加安全保护卡(例如硬盘保护卡和防毒卡,也有开机保护机制和密码机制)。
- 设置安全的口令,定期更新密码。

6. 设置安全口令的措施

1) 安全的口令

安全的口令是那些很难猜测的口令。难猜测的原因是因为同时有大小写字符,不但有字符,还有数字、标点符号、控制字符和空格。另外,还要容易记忆,至少有 8 个字符长,并且容易输入。

2) 不安全口令

不安全的口令往往是任何名字(包括人名、软件名、计算机名甚至幻想中事物的名字),电话号码或者某种执照的号码,社会保障号,任何人的生日,其他很容易得到的关于

自己的信息,一些常用的音调,任何形式的计算机中的用户名,在英语字典或者外语字典中的词,地点名称或者一些名词,键盘上的一些词,任何形式的上述词再加上一些数字。

3) 保持安全要注意下面的问题

- 不要将口令写在本子上。
- 不要将口令存于终端功能键或调制解调器的字符串存储器中。
- 不要选取显而易见的信息作口令。
- 不要将口令告诉别人。
- 不要交替使用两个口令。
- 不要在不同系统上使用同一口令。
- 自己在输入口令时不要让人看见。
- 不要永久性地使用一个口令。

4) 一次性口令

减小口令危险的最有效方法是根本不用常规口令。替代的办法是在系统中安装新的软件或硬件,使用一次性口令。一次性口令就是一个口令只使用一次。一个用户可能收到一个打印输出的口令列表,每次登录使用完一个口令,就将它从列表中删除。用户也可能得到一个可以携带的小卡,这个卡每次将显示一个不同的号。用户还可以携带一个小的计算器,当登录时,计算机将会打印出一个不同的号码,用户将这个号码输入这个小小的计算器中,然后输入自己的标志号码,计算器将输出一个口令,用户将这个口令再输入计算机中。

一次性口令系统比传统方式能提供令人惊奇的安全性能。不幸的是,它们要求安装一些特定的程序或者需要购买一些硬件,因此现在使用得并不普遍。

在一个网络中,当用户穿过 Internet 或者其他的网络来访问时,管理员就应该认真地考虑使用一次性口令。否则,攻击者可以窃听、截获用户口令,以后将攻击这些站点。

7. 口令破解实用工具 PS

文件名:PS. EXE。

功能:破解 Windows 2000/XP 及一些常规口令。

8. 口令破解实用工具 LC4SETUP

文件名:LC4SETUP. EXE。

功能:破解 Windows NT/XP 口令。

3.5 数据备份与恢复技术

随着计算机技术和网络技术的迅猛发展,无论是国外还是国内,无论是政府部门还是军事机构,也无论是国家、单位还是个人,都已离不开计算机和计算机网络,可以说,人们已开始使用计算机及网络处理一切事务,包括国家计划、军事机密、日常事务处理和家庭开支。

人们在使用计算机及网络系统处理日常业务提高工作效率的同时，系统安全、数据安全的问题也越来越突出。一旦系统崩溃或数据丢失，企业就会陷入困境。客户资料、技术文件、财务账目等数据可能被破坏得面目全非，严重时会导致系统和数据无法恢复，其结果是不堪设想的。比如 2001 年美国的“9・11 事件”，就给许多大型企业，包括一些金融机构带来了巨大的损失，其教训是深刻的。

解决上述问题的最佳方案就是进行系统及数据备份，数据备份的主要目的是一旦系统崩溃或数据丢失，就能用备份的系统和数据进行恢复，使损失减少到最小。

对计算机系统进行全面的备份，并不只是简单地进行文件备份。一个完整的系统备份方案，应由备份硬件、备份软件、日常备份制度和灾难恢复措施 4 个部分组成。选择了备份硬件和软件后，还需要根据本单位的具体情况制定日常备份制度和灾难恢复措施，并由系统管理人员切实执行备份制度。

系统备份的最终目的是保障网络系统安全、稳定、可靠地运行，所以一份优秀的网络备份方案应能够备份网络系统及其所有数据，在网络出现故障甚至损坏时，能够迅速地恢复网络系统和数据。从发现故障到完全恢复系统（含系统程序），理想的备份方案耗时不应超过半个工作日。

3.5.1 数据备份策略

1. 备份技术的 3 个层次

备份可以分为 3 个层次：硬件级、软件级和人工级。

1）硬件级备份

硬件级备份是指用冗余的硬件来保证系统的连续运行。比如磁盘镜像、双机容错等方式。如果主硬件损坏，后备硬件马上能够接替其工作，这种方式可以有效地防止硬件故障，但无法防止数据的逻辑损坏。当数据发生逻辑损坏时，硬件备份只会将错误数据复制一遍，无法真正保护数据。硬件备份的作用实际上是保证系统在出现故障时能够连续运行，硬件级备份又称为硬件容错。

2）软件级备份

软件级备份是指将系统数据保存到其他介质上，当出现错误时可以将系统恢复到备份前的状态。由于这种备份是由软件来完成的，所以称为软件备份。当然，用这种方法备份和恢复都要花费一定时间。但这种方法可以完全防止逻辑损坏，因为备份介质和计算机系统是分开的，错误不会复制到介质上，这就意味着只要保存足够长的历史数据，就能对系统及数据进行完整的恢复。

3）人工级备份

人工级备份最为原始，也最简单和有效。但如果要用手工方式从头恢复所有数据，耗费的时间恐怕会令人难以忍受。

目前采用的备份措施在硬件级备份中有磁盘镜像、磁盘阵列和双机容错等；在软件一级有数据备份。

其实，理想的备份系统是全方位、多层次的。首先，要使用硬件备份来防止硬件故

障;如果由于软件故障或人为误操作造成了数据的逻辑损坏,则使用软件方式和手工方式结合的方法恢复系统。这种结合方式构成了对系统的多级防护,不仅能够有效地防止物理损坏,还能够彻底防止逻辑损坏。

但是理想的备份系统成本太高,不易实现。在设计备份方案时,往往只选用简单的硬件备份措施,而将重点放在软件备份措施上,用高性能的备份软件来防止逻辑损坏和物理损坏。

2. 传统存储模式与现代存储模式

传统的企业业务数据存储备份和灾难恢复思想是:每天将企业业务数据备份在磁带库中,以在发生紧急情况时实现保护和恢复。但是近年来,关键数据的范围正在日益扩大,处于常规生产系统之外的电子邮件、知识产权、客户关系管理、企业计划资源、电子业务、电子商务、供应链和交易记录都存放在网络数据库中,再加上"9·11"事件之后,提出了对数据安全存储更高的要求,这种基于磁带的传统数据备份和灾难恢复模式已经不能再满足新的客户需求。因此,采用最新技术信息基础架构或存储网络的新业务连续性计划,从而将员工解放出来,转而去从事更富生产力的工作,提高人员和资源重新部署的效率,并缩短重新恢复关键性业务功能的时间成为了新的追求。

3. 异地备份

为了有效地进行灾难恢复,重要的网络系统和应用系统的数据库必须进行异地备份,这里指的"异地",指的是在两个以上不同城市甚至是不同国家之间进行热备份。比如,中国人民银行总行网络系统的中心主机设在北京,可同时在上海和广州设立实时热备份的主机,即将银行资料同时备份在3个城市的计算机上,如图3-1所示。如果北京中心主机或主机房被破坏,则可及时地从上海和广州的存储介质上恢复系统程序和数据,而且还可用广州或上海的主机代替北京中心主机继续进行银行交易活动。

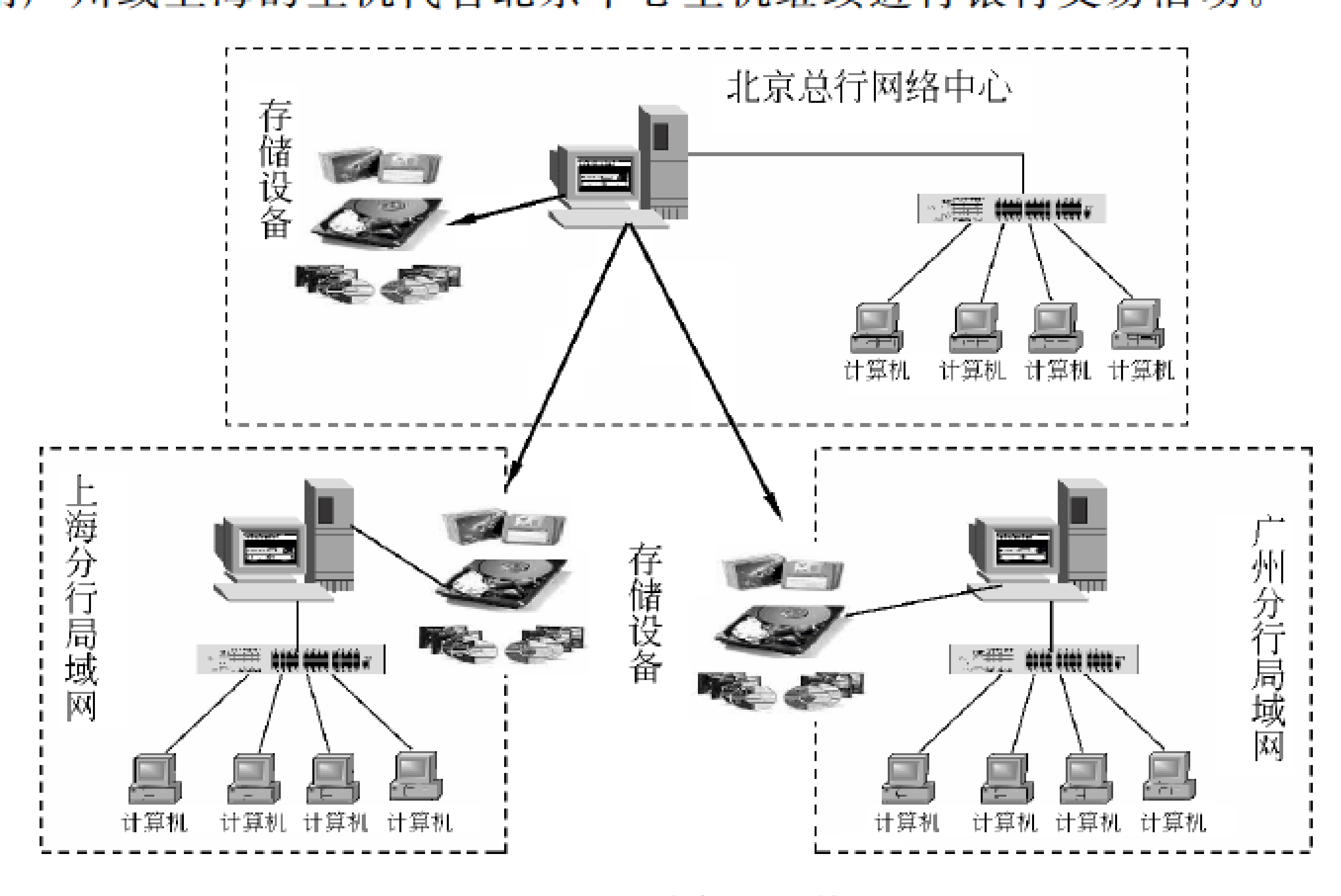


图 3-1 异地备份拓扑图

4. 高效安全的存储系统

高效安全的存储系统应综合考虑以下 3 个方面。

- 磁带的存储容量大、数据保存时间较长是其最大的优点。但磁带并非最理想的存储介质，就业务恢复流程而言，恢复磁带介质上存储的数据过程十分漫长，恢复时间往往长达几天甚至几周时间，且整个进程往往需要通过几次才能完成。这么长的恢复时间，会严重影响企业的生产和业务交易。
- 备份必须保证数据的一致性，尤其是异地备份更是如此。不一致的备份不能算备份。不连贯的数据备份会大大增加数据丢失率，数据信息可能无法实现匹配或重新组合，最终延长恢复所需的时间。
- 操作流程必须自动化。在发生严重危机时，可能因为交通道路的关闭，员工将无法前往恢复站点履行其职责。因此，理想化的 IT 环境是信息存储系统能够自动执行恢复任务，而不必开展磁带传送和载入等人为干预和人工工作。

5. 存储设备的选择

1）磁盘

磁盘是最常用的存储设备，这里所说的磁盘，指的是硬磁盘(因软盘的容量太小，一般不作为系统备份之用)，因其存取速度快，存储容量大，所以，常作为实时热备份理想的存储设备，可采用双硬盘热备份技术或磁盘阵列技术进行实时热备份。当然，也可将大容量硬盘作为非实时的系统备份之用。

2）磁带

虽然磁盘越来越普及，但作为备份工具，磁带存储仍在网络数据存储中起着重要作用。另外，还可将磁带备份存放在非现场位置，还可以保护现场数据免受病毒、火灾、自然灾害、偶然删除及其他数据丢失问题的破坏。

较之于其他存储方法，磁带具有成本低、便于从网络数据存储系统拆装、防震且经久耐用、信息稳定等诸多优点。

但磁带存储也有其不利之处。将数据转移到磁带以及将盒带移入磁带库要花一定的时间，因此这对利用磁带在限期之前完成备份的公司来说是个难题。

3）磁鼓

磁鼓的最大特点是存取速度快，可作为热备份的存储设备。磁鼓在小型计算机上用得极少，主要用在大中型计算机上。

4）光盘

光盘也是一种常用的存储备份设备，由于单张光盘的容量有限，若要用光盘作为备份介质时，最理想的是使用光盘塔。

3.5.2 数据备份技术

1. 双机热备份技术

所谓的双机热备份是一种典型的硬件冗余备份技术，其实现技术是在中心站点用两

台相同配置和性能的计算机同时运行同一套系统,其中一台作为主机,另一台作为备用主机,当主机发生故障时,系统能自动切换到备用主机上运行。保证系统运行的稳定性、可靠性和连续性。

2. 磁盘阵列技术

该技术支持在一台计算机上同时使用两块以上硬盘(一块作为主硬盘,其余的作为备用硬盘),系统运行时,多块硬盘进行同步的实时热备份。当主硬盘发生故障时,系统能自动切换到备用硬盘上工作,保证系统运行的稳定性和连续性。磁盘阵列技术的另一大特点是每一块硬盘都支持热插拔。

3. 磁盘镜像技术

将重要的系统及数据备份到本地和异地的多台计算机中,其他用户要访问这些数据时,首先到最近的镜像站点去查找,若该站点上无所需数据,再到中心站点主机上查找,如图 3-2 所示。

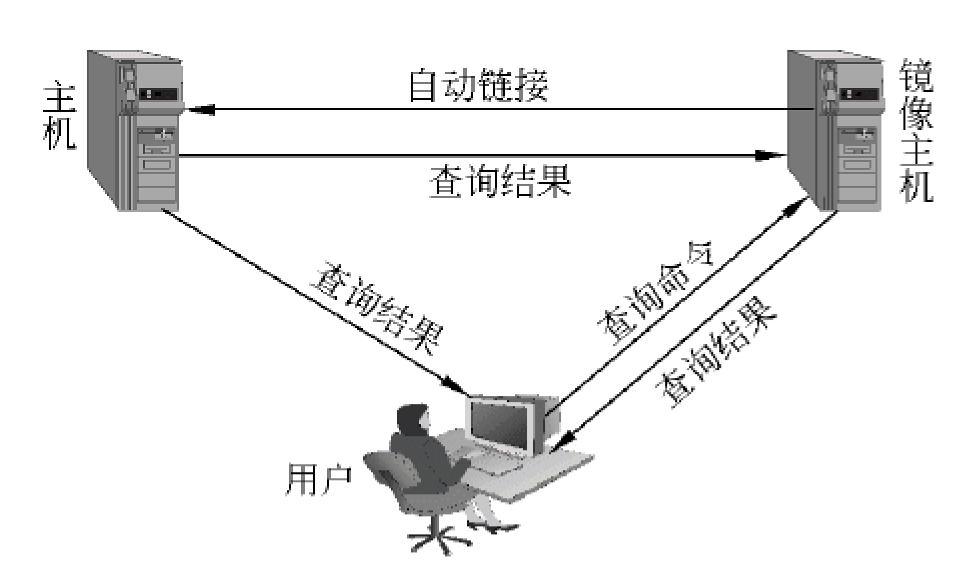


图 3-2 磁盘镜像访问技术

这种技术的优点有三个。

- 提高用户查找数据的速度和效率,节省查询时间和费用。
- 减轻中心站点主机的负担。
- 事后灾难数据恢复得到保证。

磁盘镜像技术可以同步进行实时镜像,也可事后进行镜像。同步实时镜像时要求有足够的带宽。

4. 光盘塔

一般的计算机支持的存储设备是有限的,在一台计算机上,硬盘和光驱的个数不能超过 4 个。而光盘塔则支持多张光盘,即可同时在多张光盘上存储数据。

3.5.3 网络环境数据备份技术

1. 网络数据备份系统的设计目标

前面介绍过,网络备份的最终目的是保障网络系统持续稳定地运行。为在整个网络

系统内实现全自动的数据存储管理，备份服务器、备份管理软件与智能存储设备的有机结合是这一目标实现的基础。

网络数据存储管理系统是在网络上选择一台应用服务器，将之作为网络数据存储管理服务器，在其上安装网络数据存储管理服务器端软件，作为整个网络的备份服务器。在备份服务器上连接一台大容量存储设备。在网络中其他需要进行数据备份管理的服务器上安装备份客户端软件，通过局域网将数据集中备份到与备份服务器连接的存储设备上。

网络数据存储管理系统的核心是备份管理软件，通过规划，可为企业建立完善的备份计划及策略，并可借助备份时的呼叫功能，让所有的服务器备份都能在同一时间进行。备份软件也提供完善的灾难恢复手段，能够将备份硬件的优良特性完全发挥出来，使备份和灾难恢复时间大大缩短，实现网络数据备份的全自动智能化管理。

灾难恢复的先决条件是要做好备份策略及恢复计划。日常备份制度描述了每天的备份以什么方式、使用什么备份介质进行，是系统备份方案的具体实施细则。在备份方案制订完毕后，应严格按照制度进行日常备份，否则将无法达到备份方案的目标。

2. 网络数据备份策略

网络数据存储管理系统是指在分布式网络环境下，通过专业的数据存储管理软件，结合相应的硬件和存储设备，来对全网络的数据备份进行集中管理，从而实现自动化的备份、文件归档、数据分级存储以及灾难恢复等。

网络数据备份有多种方式，其备份技术有全备份、增量备份和差分备份。

1）全备份（full backup）

所谓全备份就是用一盘磁带对整个系统进行完全备份，包括系统和数据。这种备份方式的好处就是很直观，容易被人理解。而且当发生数据丢失的灾难时，只要用一盘磁带（即灾难发生之前的备份磁带），就可以恢复丢失的数据。然而它也有不足之处：首先由于每天都对系统进行完全备份，因此在备份数据中有大量是重复的，例如操作系统与应用程序。这些重复的数据占用了大量的磁带空间，这对用户来说就意味着增加成本；其次，由于需要备份的数据量相当大，因此备份所需时间较长。对于那些业务繁忙，备份窗口小的用户来说，选择这种备份策略无疑是不明智的。

2）增量备份（incremental backup）

增量备份技术是每次备份的数据是相对于上一次备份后增加的和修改过的数据。这种备份的优点很明显，没有重复的备份数据，既节省了磁带空间，又缩短了备份时间。但它的缺点在于当发生灾难时，恢复数据比较麻烦。如果系统发生了故障，丢失大批数据，需要将系统恢复。这时管理员必须找出每一天的备份磁带，一天一天地进行恢复。很明显这比全备份策略麻烦得多。另外这种备份可靠性也差。在这种备份下，各磁带间的关系就像链子一样，一环套一环，其中任何一盘磁带出了问题都会导致整条链子脱节。

3）差分备份（differential backup）

差分备份就是每次备份的数据是相对于上一次全备份之后新增加的和修改过的数

据。管理员先在星期一进行一次系统完全备份;然后,管理员再将当天所有与星期一不同的数据(新建的或更改的)备份到磁带上。举例来说,在星期一,网络管理员进行系统完全备份;在星期二,假设系统内只多了一份"资产清单",于是管理员只需将这份"资产清单"备份下来即可;在星期三,假设系统内又多了一份"产品目录",于是管理员要将这份"产品目录"连同星期二的那份"资产清单"一并备份下来。如果在星期四系统内又多了一张"工资表",那么星期四需要备份的内容就是"工资表+产品目录+资产清单",如图 3-3 所示。

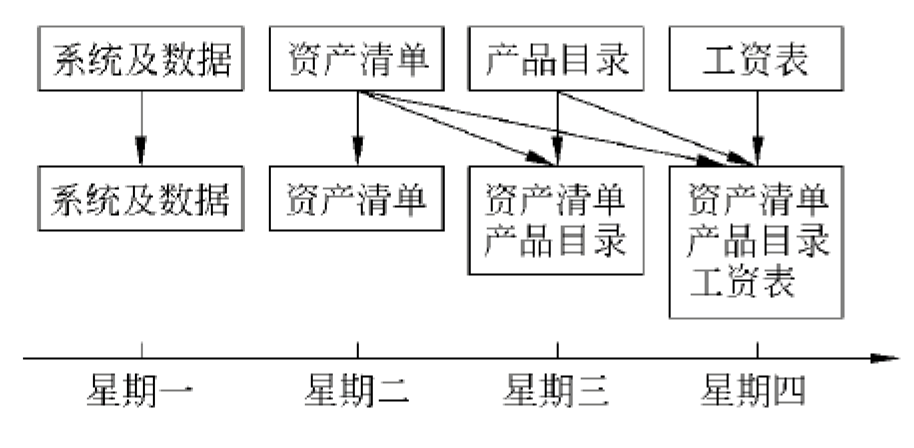


图 3-3 差分备份技术

由此可以看出,全备份所需时间最长,但恢复时间最短,操作最方便,当系统中数据量不大时,采用全备份最可靠;差分备份在避免了另外两种策略缺陷的同时,又具有了它们的所有优点。首先,它无需每天都做系统完全备份,因此备份所需时间短,并节省磁带空间;其次,它的灾难恢复也很方便,系统管理员只需两盘磁带,即星期一的磁带与发生前一天的磁带,就可以将系统完全恢复。我们在备份时要根据它们各自的特点灵活使用。

灾难恢复措施在整个备份制度中占有相当重要的地位。因为它关系到系统、软件与数据在经历灾难后能否迅速恢复如初。全盘恢复一般应用在服务器发生意外灾难导致数据全部丢失、系统崩溃或是有计划的系统升级、系统重组等,也称为系统恢复。随着备份设备应用技术的高速发展,惠普于 1999 年 5 月就推出了拥有单键恢复(OBDR)功能的磁带机,只需先用系统盘引导机器启动,将磁带插入磁带机,按动一个按键即可将整个系统恢复如初。单键恢复(又叫一键恢复)的技术将成为现在和将来备份技术的主流。

3. 数据备份方式

- 自动备份进程由备份服务器承担。每天晚上,自动按照事先制订的时间表所要求内容,进行增量或全备份。
- 批前及批后备份。在主机端,由批处理人员输入触发备份命令,自动按要求备份数据库有关内容。
- 其他文件的自由备份。进入软件交互菜单,选择要求备份的文件后备份。
- 在线跟踪备份。配合数据存储管理软件的数据库在线备份功能,可定义实时或定时将日志备份。
- 灾难备份异地存放介质的克隆。自动复制每日完成后的数据,并进行异地备份以作灾难恢复。

4. 理想的网络备份方法

在网络系统安全建设中，必不可少的一个环节就是数据的常规备份和历史保存。一般来说，本地备份的目的主要有两个，一个是及时在本地实现数据的恢复；另一个在发生地域性灾难时，及时在本地或异地实现数据及整个系统的灾难恢复。此外，更应建立历史归档数据的异地存放制度，确保对历史业务数据可靠恢复与有效稽核的实现。

综上所述，理想的网络备份系统应该具备以下功能：

- 集中式管理。利用集中式管理，系统管理员可对全网的备份策略进行统一管理，备份服务器可以监控所有机器的备份作业，也可以修改备份策略，及时浏览所有目录。
- 全自动的备份。备份系统能根据用户的实际需求，定义需要备份的数据，然后以图形界面方式根据需要设置备份时间表。备份系统将自动启动备份作业，无需人工干预。
- 数据库备份和恢复。如果数据库系统是基于文件系统的，可以用备份文件的方法备份数据库。目前的数据库系统都相当复杂和庞大，是否能够将需要的数据从庞大的数据库文件中抽取出来进行备份，是网络备份系统是否先进的标志之一。
- 在线式索引。备份系统应为每天的备份在服务器中建立在线式索引，当用户需要恢复时，只需选取在线式索引中需要恢复的文件或数据，该系统就会自动进行文件的恢复。
- 归档管理。用户可以按项目、时间，定期对所有数据进行有效的归档处理。提供统一的 Open Tape Format 数据存储格式，从而保证所有的应用数据由一个统一的数据格式来做永久的保存，以保证数据的永久可利用性。
- 有效的媒体管理。备份系统对每一个用于作备份的磁带自动加入一个电子标签，同时在软件中提供识别标签的功能，只需执行这一功能，就能迅速知道该磁带的内容。
- HSM 分级存储管理。对出版业、制造业等易产生大量资料数据的行业而言，资料多属于极占空间的图形影像，且每张设计底稿及文件资料又常需随时保持在线状态，分级存储管理（Hierarchical Storage Management，HSM）系统是一个合适的在线备份解决方案。
- 系统灾难恢复。网络备份的最终目的是保障网络系统能持续、稳定地运行。所以优秀的网络备份方案应能够备份系统的关键数据，在网络出现故障甚至损坏时，能够迅速地恢复网络系统。
- 满足系统不断增加的需求。备份软件必须能支持多平台系统，当网络上连接了其他的应用服务器时，只需在其上安装支持这种服务器的客户端软件即可将数据备份到磁带库或光盘库中。

3.5.4 灾难恢复技术

局域网环境下的系统恢复，绝非备份数据和故障后恢复那么简单。一个完备的局域

网灾难恢复策略，应当对影响局域网正常运转的所有事件有相应的策略。从根本上说，这种恢复策略应当包括 3 个重要部分：数据保护、灾难防备和事后恢复。

1. 备份软件

对保护数据来说，功能完善、使用灵活的备份软件必不可少。合格的备份软件应当具有以下功能。

- 保证备份数据的完整性，并具有对备份介质（比如磁带）的管理能力。数据完整性是系统恢复后立即可用的前提，因此，只有保证数据完整性，数据备份才有意义。超大系统的备份介质管理需要备份软件的参与和支持。特别是，备份软件需要具有"通知机制"，可以提醒系统管理员何时更换备份介质，何时从备份设备中取出备份介质，为系统管理员建议介质轮换周期、备份策略。
- 支持多种备份方式，可以定时自动备份。除了支持常规备份方式（完全式、增量式和差分式）以外，还可以设置备份自动启动和停止的日期，记录系统配置以供重用，处理备份中的各种情况。
- 具有相应的功能或工具，进行设备管理、介质管理。这种功能或工具应当支持各种类型的介质，包括级联式磁带、磁带库、磁带组和磁带阵列等。备份软件应当保存设备和介质活动记录，诸如磁带首次格式化的时间、格式化次数。
- 支持多种校验手段，以保证备份的正确性。备份软件至少应当提供字节校验、CRC（循环冗余校验）校验和快速磁带扫描等手段。还应该提供磁带到磁带的复制和比较功能，并对写入磁带的数据提供保护。
- 提供联机数据备份功能。在联机状态下进行数据备份对许多系统都是一大挑战。但是，合格的备份软件必须具备这一功能，因为对依靠数据库服务器管理数据的应用系统来说，这一功能必不可少。

除了以上功能外，更完善的备份软件还支持 RAE 磁带容错技术和图像备份功能。前者保证个别磁带遭到破坏时，整个备份仍然可用。后者使用户可以绕开系统，对图像快速备份。

2. 恢复的选择和实施技术

数据备份只是系统成功恢复的前提之一。恢复数据还需要备份软件提供各种灵活的恢复选择，如按介质、目录树、磁带作业或查询子集等不同方式做数据恢复。此外，还要认真完成一些管理工作，定期检查，确保备份的正确性；将备份磁带保存在异地一个安全的地方（如专门的磁带库或银行保险箱），按照数据增加和更新速度选择恰当的备份周期。一般而言，部分备份周期不应该超过一个月。

服务器的保护对客户机/服务器环境而言，传统的针对大型主机的恢复策略是不适用的。客户机/服务器环境恢复的关键是保护好服务器管理的数据。而服务器磁盘的安全有效又是保护数据的关键。因此，配备高性能、具有容错能力的磁盘存储器，是保护服务器的有力措施之一。

3. 灾难恢复

灾难恢复措施在整个备份制度中占有相当重要的地位。因为它关系到系统在经历灾难后能否迅速恢复。灾难恢复操作通常可以分为两类，全盘恢复和个别文件恢复。还有一种就是重定向恢复。

- 全盘恢复。全盘恢复又称系统恢复，一般应用在服务器发生意外灾难时导致数据全部丢失、系统崩溃，或是有计划的系统升级、系统重组等。
- 个别文件恢复。个别文件恢复要比全盘恢复常见得多。利用网络备份系统的恢复功能，很容易恢复受损的个别文件。只需浏览备份数据库或目录，找到该文件，触发恢复功能即可。
- 重定向恢复。重定向恢复是将备份的文件恢复到另一个不同的位置或系统上去。重定向恢复可以是整个系统恢复，也可以是个别文件恢复。重定向恢复时需要慎重考虑，要确保系统或文件恢复后的可用性。

4. 自启动恢复

系统灾难通常会使企业丢失数据或者无法使用数据。利用备份软件可以恢复丢失的数据，但是，重新使用数据并非易事。很显然，要想重新使用数据并恢复整个系统，首先必须将服务器恢复到正常运行状态。为了提高恢复效率、减少服务停止时间，应当使用“自启动恢复”软件工具。通过执行一些必要的恢复功能，自启动恢复软件可以确定服务器需要的配置和驱动。因此，无须重新人工安装、配置操作系统，也不需要重新安装、配置磁带恢复软件及应用程序。此外，自启动恢复软件还可以生成备用服务器的数据集和配置信息，以简化备用服务器的维护。

5. 病毒防护

如果系统中潜伏着病毒，那么即使数据和系统配置没有丢失，服务器中的数据也不能保证其正确性。因此，病毒防护也是灾难恢复的重要内容。在数据和程序进入网络之前，要作病毒的检验和清除处理。更为重要的是，要对整个网络自动监控，防止新病毒出现和传播。这些功能只有在强大的防病毒软件支持下才能实现。防病毒软件应该与其他防灾方案密切配合，同时互相透明。总而言之，一个完整的灾难恢复方案必须包括很强的病毒防护策略和技术手段。

6. 异地容灾技术

异地容灾技术的核心就在于在不同的地方将灾难化解，在实践中主要表现为两个方面：一是保证企业数据的安全，二是保证业务的连续性。由于工作站点和灾难恢复站点运行同样的系统，包括操作系统、基础数据库和应用软件，并通过数据复制管理器完成在线和实时的本地复制，或者通过光纤通道的远程数据复制。假如工作站点发生灾难，不能再继续工作，这时容灾中心会将业务数据及时恢复到备用服务器上，并自动将业务切换到备用服务器，然后实现业务的远程切换，恢复系统不间断的运行，在容灾中心实现应

用的异地容灾,这个过程只需要几秒或者几分钟的时间。

由于异地容灾的核心就是在工作站点以外的地方将灾难化解,所以异地容灾解决方案的基本原理就是在工作站点一定距离之外设立灾难恢复站点,然后通过网络设备将生产站点和灾难恢复站点连接起来,以实现实时的数据同步。异地容灾解决方案以存储区域网络为基础,在存储区域网络与网络之间采用光纤通道交换技术来实现连接。

异地容灾系统的关键技术包括网络技术、存储技术及解决方案。从网络层面而言,无论是 ATM 网络还是光纤网络,都已经在世界各地得到了广泛的应用;在存储技术方面,磁盘阵列(Redundant Arrays of Independent Disks,RAID)技术已经成熟,磁盘阵列的应用已经遍布全球每一个角落;存储区域网络在世界各地也得到了全面的认同。

一般来说,异地容灾的技术分为两种。

- 基于主机系统的数据恢复是通过软件形式来实现的,目前各大数据库厂商都是通过这种方法实现对数据库中数据的备份。有关数据安全性方面的公司,比如像 IBM、VERITAS 都推出了一系列的跨平台存储管理软件的解决方案。基于主机系统的数据复制能够把数据定期、在线地复制到目的地的机器上去。对用户来说,这种复制方式的优点是能够较好地保证数据的一致性,但它将消耗大量的主机资源,这种方式要求做任何一笔交易,都要实时地将结果发送到远程的站点中,等待远程操作结束后,再执行下一笔交易。在实际操作中,很难做到这一点,只能做异步的数据复制。
- 基于智能存储系统的远程镜像。这种方法是基于控制器的远程复制,具有在主副存储子系统之间同步数据镜像的能力,对主机的资源占用很小,能保证业务正常运行下的 I/O 响应。但缺点是会受通信链路的通信条件的影响。当带宽不够的时候,只能做远程的异步复制。

用户如何选择这两种技术呢?比较而言,由于基于智能存储的远程复制是通过硬件实现复制,其稳定性优于基于主机系统的复制,但在灵活性和兼容性上要差一些。

在企业的一些中低端应用中,当成本预算较紧、主机资源又不是瓶颈的情况下,可以考虑选用基于主机系统的通过软件实现复制的方法;而对于企业中的一些关键应用,比如银行业务、电信计费、大型企业业务以及政府的办公系统数据等,由于可靠性要求高,业务不能中断,需要选用针对企业的高端应用的容灾解决方案。

习 题 3

1. 国际上对计算机安全的定义是什么?
2. 计算机系统的安全保护技术有哪些?
3. 软件的集中式管理方式的优缺点分别是什么?
4. CMOS 口令的破解方法有哪几种?
5. 数据备份的层次是如何划分的?
6. 网络数据备份技术有哪几种?
7. 全备份、增量备份和差分备份各自的功能是什么?
8. 在数据备份技术中,什么是重定向恢复技术?

第 4 章 chapter 4

信息安全技术

4.1 信息安全技术概述

当今世界是信息的时代，通信技术、计算机技术和计算机网络技术的迅猛发展大大提高了信息的获取、处理、传输、存储和应用能力，信息数字化已经成为普遍现象。随着互联网的普及和应用，更方便了信息的共享和交流，使信息技术的应用已经扩展到社会经济、政治、军事、个人生活等各个领域。因此，信息安全的重要性可以上升到国家安全的高度。可以说，当今的社会，已离不开计算机网络，更离不开信息。因此，学习和掌握好信息安全知识，掌握好计算机网络安全技术，是人们的当务之急。

4.1.1 信息安全的目标

信息安全的目标是保护信息的机密性、完整性、真实性、抗否认性、可用性和访问控制。通常将机密性、完整性和可用性称为 CIA 技术。

保护信息的机密性有两个含义，其一是阻止非授权用户非法访问和获取信息，即保证信息不被非授权访问；其二是对信息进行加密处理，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容。

1. 完整性服务

完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。

2. 机密性服务

将系统中的敏感信息进行秘密传输或存储，保证消息的机密性，根据消息内容的结构，可以将保密服务实施在不同的层次上。最常用的保密服务是在特定的时间段内保护两个用户之间传输的所有消息不发生泄露。

3. 抗否认服务

抗否认服务又称抗赖服务,指的是能保障用户无法在事后否认曾经对信息进行的生成、签发和接收等行为,是针对通信各方信息真实性的安全要求。一般通过数字签名和身份认证技术来提供抗否认服务。抗否认服务在电子商务的应用中起着非常重要的作用。

4. 可用性服务

可用性是指保障信息资源随时可提供服务的特性,即授权用户根据需要可以随时访问所需信息。可用性是信息资源服务功能和性能可靠性的度量,涉及物理、网络、系统、数据、应用和用户等多方面的因素,是对信息网络总体可靠性的要求。

5. 真实性服务

消息认证用于保证消息的真实性,在消息单向传输中,认证的功能是使消息的接收者相信消息确实来源于该消息所声明的信源。在双向传输中,认证服务涉及通信双方,在连接发起时,认证服务确保通信双方身份的真实性。在连接建立后认证服务还应该保证该连接不被第三方假冒。

6. 访问控制

在网络环境中,访问控制的目的是限制用户对网络资源的非授权访问。每个试图访问网络的实体都必须识别其身份,身份得到鉴别后即可获得为其定制的访问权限。同时还应该对各合法用户的访问权实施授权、保密、变更和收回等管理服务。

4.1.2 信息加密与信息安全

信息安全是一门交叉学科,涉及多方面的理论和应用知识。除了数学、通信和计算机等自然科学外,还涉及法律、心理学等社会科学。

信息安全研究可分为基础理论研究、应用技术研究和安全管理研究等几个方面。

- 基础理论研究包括密码研究、安全理论研究。
- 应用技术研究包括安全实现技术、安全平台技术研究。
- 安全管理研究包括安全标准、安全策略、安全测评研究。

在本节中,介绍的是密码理论及加密应用技术。

1. 密码理论

密码理论(cryptography)是信息安全的基础,信息安全的机密性、完整性和抗否认性都依赖于密码算法。通过信息加密技术保护信息的机密性;通过信息摘要技术检测信息的完整性;通过数字签名技术保护信息的抗否认性。加密变换需要密钥,因为任何人只要拥有了密钥就能轻而易举地破译用户的密文,所以,密钥的保护、传输与管理是十分重要的研究内容。因此,密码学的主要研究内容是加密算法、消息摘要算法、数字签名算法

以及密钥管理技术。

1）数据加密（data encryption）

数据加密算法是对明文实施一种数学变换，用选定参数（密钥），将信息从易于理解的明文加密为不易理解的密文，同时也可以将密文解密为明文。加、解密时用的密钥可以相同，也可以不同。加、解密密钥相同的算法称为对称算法，或称为对称密钥体制，典型的对称加密算法有 DES、AES 等；加、解密密钥不同的算法称为非对称算法，通常一个密钥公开，另一个密钥私藏，因而也称为公开密钥算法，简称为公钥算法，典型的公钥算法有 RSA、ECC 等。

2）消息摘要（message digest）

消息摘要算法并不对整个消息正文进行加密，而只对摘要内容进行加密，其目的是缩短消息加密的时间，提高数据的传输效率。消息摘要算法也是一种数学变换，通常是单向（不可逆）的变换，它将不定长度的信息变换为固定长度（如 64 位或 128 位）的摘要，信息的任何改变（即使是 1b）也能引起摘要内容的面目全非，因而可以通过消息摘要检测消息在传输过程中是否被篡改。典型的消息摘要算法有 MD5、SHA 等。

3）数字签名（digital signature）

数字签名技术是消息摘要算法和非对称加密算法的有机结合与应用。从原理上讲，通过私有密钥用非对称算法对信息本身进行加密，即可实现数字签名功能。用私钥加密只能用公钥解密，使得接受者可以解密信息，但无法生成用公钥解密的密文，从而证明此密文肯定是拥有加密私钥的用户所为，因而是不可否认的。实际实现时，由于非对称算法加/解密速度很慢，通常先计算消息摘要，再用非对称加密算法对消息摘要进行加密而获得数字签名。

4）密钥管理（key management）

密码算法是可以公开的，但密钥必须严格保护。如果非授权用户获得加密算法和密钥，则很容易破解或伪造密文，信息加密也就失去了意义。密钥管理研究就是研究密钥的产生、发放、存储、更换和销毁的算法和协议。

2. 信息安全技术

1）身份认证（authentication）

身份认证是指验证用户身份与其所声称的身份是否一致的过程。最常见的身份认证是口令认证。口令认证是在用户注册时记录下其用户名和口令，在用户请求服务时出示用户名和口令，通过比较其出示的用户名和口令与注册时记录下的是否一致来鉴别身份的真伪。复杂的身份认证则需要基于可信的第三方权威认证机构的保证和复杂的密码协议来支持，如基于证书认证中心（CA）和公钥算法的认证等。

身份认证研究的主要内容包括认证的特征（知识、推理和生物特征等）和认证的可信协议及模型。

2）授权和访问控制（authorization and access control）

授权和访问控制是两个关系密切的概念，常常替换使用。它们的差别在于，授权侧重于强调用户拥有什么样的访问权限，这种权限是系统预先设定的，并不关心用户是否

发起访问请求;而访问控制是对用户访问行为进行控制,它将用户的访问行为控制在授权允许的范围之内,因此,也可以说,访问控制是在用户发起访问请求时才起作用的。打个形象的比喻,授权是签发通行证,而访问控制则是卫兵,前者规定用户是否有权出入某个区域,而后者检查用户在出入时是否超越了禁区。

授权和访问控制研究的主要内容是授权策略、访问控制模型、大规模系统的快速访问控制算法等。

3) 审计追踪(auditing and tracing)

审计和追踪也是两个关系密切的概念,审计是指对用户的行为进行记录、分析和审查,以确认操作的历史行为。追踪则有追查的意思,通过审计结果追查用户的全程行踪。审计通常只在某个系统内进行,而追踪则需要对多个系统的审计结果综合分析。

审计追踪研究的主要内容是记录方式、审计模型及追踪算法等。

4) 安全协议(security protocol)

安全协议是指在构建安全平台时所使用的与安全防护有关的协议,是各种安全技术和策略具体实现时共同遵循的规定,如安全传输协议、安全认证协议和安全保密协议等。典型的安全协议有网络层安全协议 IPSec、传输层安全协议 SSL 和应用层安全电子商务协议 SET 等。

安全协议研究的主要内容是协议的内容和实现层次、协议自身的安全性以及协议的互操作性等。

4.1.3 经典加密技术

1. 几个术语

- 经典加密技术。经典加密技术又叫传统加密技术。
- 密码学。密码学研究的是密码编码学和密码分析学的科学。
- 密码编码学。是对信息进行编码实现信息保密性的科学。
- 密码分析学。是研究、分析、破译密码的科学。
- 单密钥系统。单密钥系统又称为对称密码系统或秘密密钥密码系统,单密钥系统的加密密钥和解密密钥或者相同,或者实质上等同,即易于从一个密钥推出另一个密钥。
- 双密钥系统。双密钥系统又称为非对称密码系统或公开密钥密码系统。双密钥系统有两个密钥,一个是公开密钥,是大家都可以使用的密钥,另一个是私有密钥,只能是该密钥拥有者才能使用,而且从公开密钥是推不出私有密钥的。
- 经典密码体制。经典密码体制是传统的加密解密体制,采用手工或机械操作实现加/解密。经典密码大体上可分为三类,单表代换密码、多表代换密码和多字母代换密码。

2. 单表代换密码

将字母 a、b、c、d、…、w、x、y、z 用 d、e、f、g、…、z、a、b、c 来代替(即将字母表中的每个

字母用其后的第 3 个字母进行替换，此时密钥为 3）。例如，若明文为 student，则对应的密文为 vwxghqw。这就是著名的恺撒(Kaesar)密码，也称为移位代换密码。

恺撒密码仅有 26 个可能的密钥，是不安全的。如果允许字母表中的字母用任意字母进行替换（“随机置换”加密算法），即上述密文能够是 26 个字母的任意排列，则将有 26！或多于 4×10^{26} 种可能的密钥。这样的密钥空间既使用计算机进行穷举搜索密钥也是不现实的。

例 4-1 “随机”置换加密与解密算法。

明文：a b c d e f g h i j k l m n o p q r s t u v w x y z

密文：X N Y A H P O G Z Q W B T S F L R C V M U E K J D I

解密是如下的一个逆置换。

密文：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

明文：d l r y v o h e z x w p t b g f j q n m u s k a c i

设接收方收到这样一条密文：

MGZV YZLGHC MHJM YXSSFM NH AHYCDLMHA

根据例 4-1 的密钥约定，其解密后的明文如下：

this cipher text cannot be decrypted

3. 多表代换密码

多表代换密码中最著名的一种密码称为维吉尼亚(Vigenere)密码。这是一种以移位代换为基础的周期代换密码，m 个移位代换表由 m 个字母组成的密钥字确定（这里假设密钥字中 m 个字母不同，如果有相同的，则代换表的个数是密钥字中不同字母的个数）。如果密钥字为 deceptive，明文为“we are discovered save yourself”的加密过程为：

字母：a b c d e f g h i j k l m n o p q r s t u v w x y z

数码：0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

明文：w e a r e d i s c o v e r e d s a v e y o u r s e l f

密钥：d e c e p t i v e d e c e p t i v e d e c e p t i v e

移位：3 4 2 4 15 19 8 21 4 3 4 2 4 15 19 8 21 4 3 4 2 4 15 19 8 21 4

密文：Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

其中，密钥字母 a、b、…、y、z 对应数码 0、1、…、24、25。这里的数码就是在加密过程中对应字母向右（后）移位的位数，由此位对应的字母即为替换字母。

加密过程是，密钥字母 d 对应数字 3，因而明文字母 w 在密钥字母 d 的作用下向右（后）移 3 位，得到密文字母 Z；明文字母 e 在密钥字母 e 的作用下向右（后）移 4 位，得到密文字母 i，以此类推。解密时，密文字母在密钥字母的作用下向左（前）移位。

分析：在维吉尼亚密码中，如果密钥字的长度是 m，明文中的一个字母是能够映成这 m 个字母中的一个的。容易看出，维吉尼亚密码中长度为 m 的可能密钥字的个数是 26^m，甚至对于一个较小的 m 值，如 $m=5$，密钥空间为 26^5，超过了 1.1×10^7，这个空间已经足以阻止手工穷举密钥搜索。但这么大的密钥空间，若用计算机进行穷举搜索，是毫

不费力的，只要几分钟时间，所以，若要抗击计算机穷举分析，则需 $m \geq 8$。

为方便记忆，维吉尼亚密码的密钥字常常取自于英文中的一个单词、一个句子或一段文章。因此，其明文和密钥字母频率分布仍然能够用统计分析技术进行统计分析攻击。要抗击这样的密码分析，只有选择没有统计关系的密钥内容。1918 年美国的 G. W. Vernam 提出的密码理论是，明文英文字母编成 5 比特二元数字，称之为 5 单元波多代码(baudot code)，选择随机二元数字流作为密钥，加密通过执行明文和密钥的逐位异或操作，产生密文，可以简单地表示为 $C_i = P_i \oplus K_i (i=1,2,3,4,5)$，这就是 Vernam 加密技术。

其中，P_i表示明文的第 i 个二元数字，K_i表示密钥的第 i 个二元数字，C_i表示密文的第 i 个二元数字，"⊕"表示异或操作。解密仅需执行相同的逐位异或操作 $P_i = C_i \oplus K_i$。

Vernam 密码系统的密钥若不重复使用，就能得到一次一个密码。若密钥有重复，尽管使用长密钥增加了密码分析的难度，但只要有了足够的密文，使用已知的或可能的明文序列，或二者相结合就能够破译。

例 4-2 Vernam 密码系统的应用。

设明文为：it is a dog

明文对应的数码为：8 19 8 18 0 3 14 6

设密钥为：deceptive

密钥对应的数码为：3 4 2 4 15 19 8 21 4

则密文为：lxkwpqgt

其加密过程如下：

第 1 步，按维吉尼亚方法将字母按顺序列表如表 4-1 所示。

表 4-1 Baudot 代码表

字　母	数　码	波多代码	字　母	数　码	波多代码	字　母	数　码	波多代码
a	0	00000	j	9	01001	s	18	10010
b	1	00001	k	10	01010	t	19	10011
c	2	00010	l	11	01011	u	20	10100
d	3	00011	m	12	01100	v	21	10101
e	4	00100	n	13	01101	w	22	10110
f	5	00101	o	14	01110	x	23	10111
g	6	00110	p	15	01111	y	24	11000
h	7	00111	q	16	10000	z	25	11001
i	8	01000	r	17	10001			

第 2 步，按 Vernam 加密方法，将明文"it is a dog"进行加密，其加密过程如表 4-2 所示。在表 4-2 中，密文对应的数码＝明文对应的数码⊕密钥对应的数码。

表 4-2 Vernam 加密过程

序 号	明 文	明文对应的数码	密 钥	密钥对应的数码	密文对应的数码	密 文
1	i	01000	d	00011	01011	l
2	t	10011	e	00100	10111	x
3	i	01000	c	00010	01010	k
4	s	10010	e	00100	10110	w
5	a	00000	p	01111	01111	p
6	d	00011	t	10011	10000	q
7	o	01110	i	01000	00110	g
8	g	00110	v	10101	10011	t

在表 4-2 中的“密文”字母用“密文对应的数码”查表 4-1 所得。

4. 多字母代换密码

前面介绍的密码都是以单个字母作为代换的对象，对多于一个字母进行代换，就是多字母代换密码。它的优点是容易将字母出现的频度隐蔽，从而抗击统计分析。这里介绍 Hill 密码，它是数学家 Lester Hill 于 1929 年研制的。虽然这类密码由于加密操作复杂而未能广泛应用，但仍在很大程度上推进了经典密码学的研究。

Hill 密码将明文分成每 m 个字母为一组的明文组，若最后一组不够 m 个字母就用字母补足，每组用 m 个密文字母代换，这种代换由 m 个线性方程决定，其中字母 a、b、…、y、z 分别用数字 0、1、…、24、25 表示。若 $m=3$，该系统可以描述如下：

$$C_1 = (k_{11}P_1 + k_{12}P_2 + k_{13}P_3) \bmod 26$$
$$C_2 = (k_{21}P_1 + k_{22}P_2 + k_{23}P_3) \bmod 26$$
$$C_3 = (k_{31}P_1 + k_{32}P_2 + k_{33}P_3) \bmod 26$$

可用列向量和矩阵表示为：

$$\begin{pmatrix} \boldsymbol{C}_1 \\ \boldsymbol{C}_2 \\ \boldsymbol{C}_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} \boldsymbol{P}_1 \\ \boldsymbol{P}_2 \\ \boldsymbol{P}_3 \end{pmatrix}$$

或

$$\boldsymbol{C} = \boldsymbol{KP}$$

其中，$\boldsymbol{C}$ 和 $\boldsymbol{P}$ 分别是密文和明文向量，$\boldsymbol{K}$ 是密钥矩阵，注意操作过程要执行模 26 运算。

例 4-3 用密钥

$$\boldsymbol{K} = \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix}$$

来加密明文 july。将明文分成两个组 ju 和 ly，分别为(9,20)和(11,24)，计算如下：

$$\begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 9 \\ 20 \end{pmatrix} = \begin{pmatrix} 99 + 60 \bmod 26 \\ 72 + 140 \bmod 26 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix}11 & 3\\ 8 & 7\end{pmatrix}\begin{pmatrix}11\\ 24\end{pmatrix}=\begin{pmatrix}121+72 \bmod 26\\ 88+168 \bmod 26\end{pmatrix}=\begin{pmatrix}11\\ 22\end{pmatrix}$$

因此,july 的加密结果为 delw。

为了解密,必须先计算密钥矩阵 $\boldsymbol{K}$ 的逆矩阵。

$$\boldsymbol{K}^{-1}=\begin{pmatrix}7 & 23\\ 18 & 11\end{pmatrix}$$

然后计算 $\boldsymbol{P}=\boldsymbol{K}^{-1}\boldsymbol{C}$

$$\begin{pmatrix}7 & 23\\ 18 & 11\end{pmatrix}\begin{pmatrix}3\\ 4\end{pmatrix}=\begin{pmatrix}21+92 \bmod 26\\ 54+44 \bmod 26\end{pmatrix}=\begin{pmatrix}9\\ 20\end{pmatrix}$$

$$\begin{pmatrix}7 & 23\\ 18 & 11\end{pmatrix}\begin{pmatrix}11\\ 22\end{pmatrix}=\begin{pmatrix}77+506 \bmod 26\\ 198+242 \bmod 26\end{pmatrix}=\begin{pmatrix}11\\ 24\end{pmatrix}$$

最后,得到正确的明文 july。

从以上分析知道,单表代换密码和多表代换密码都是每次加密一个字母,而多字母代换密码每次可加密多个字母。

4.1.4 现代加密技术

现代密码理论起源于 20 世纪 70 年代,但其理论基础可以追溯到 1949 年 Shanon 的论文“保密通信的理论基础”。现代密码理论充分结合了数学理论基础和计算机计算能力,提出了密码算法的框架结构。其标志性的成果首推 DES 算法和 RSA 算法。

数据加密标准 DES(Data Encryption Standard)是 1977 年美国国家标准局正式公布实施的。该算法在此后几年中一直作为国际最通用的分组加密算法在使用。虽然后来出现了其改进算法 3DES,但除了增加了 DES 加解密的运算次数和顺序外,没有本质的突破。DES 算法将数据按 64 位分组进行加密,其密钥长度也是 64 位,其中每 8 位中有一位校验位,因此 DES 的有效密钥长度为 56 位。DES 不仅仅是一个加密算法,它还代表了现代对称密码算法的一般性结构,后来很多算法都是在 DES 结构上发展起来的。

现代密码的另一个标志就是公钥密码体制的提出。Diffie 和 Hellman 在《密码学的新方向》中首次提出了非对称密码算法的思想。两年后 Rivest、Shamir 和 Adleman 提出的 RSA 算法体现了公钥算法的思想。RSA 算法至今仍然是公钥密码算法的典型代表。

目前,密码学的研究依然炙手可热,美国花巨资历时 3 年挑选了代替 DES 算法的 AES 算法,欧洲也正在制定新的欧洲密码体制。在公钥体制方面,椭圆曲线算法 ECC 是目前研究的热点。

对称密码体制根据对明文加密方式的不同而分为分组密码和流密码。前者按一定长度(如 64 字节、128 字节等)对明文进行分组,然后以组为单位进行加/解密;后者则不进行分组,而是按位进行加/解密。

1. 分组密码原理

分组密码系统对不同的组采用同样的密钥 k 来进行加/解密。设密文组为

$y=y_1y_2\cdots y_n$，则对明文组 $x=x_1x_2\cdots x_n$ 用密钥 k 加密可得到 $y=e_k(x_1)e_k(x_2)\cdots e_k(x_n)$，如图 4-1所示。

流密码的基本思想是利用密钥 k 产生一个密钥流 $z=z_0z_1\cdots$，并使用如下规则加密明文串 $x=x_0x_1x_2\cdots$，$y=y_0y_1y_2\cdots=e_{z0}(x_0)e_{z1}(x_1)e_{z2}(x_2)\cdots$。密钥流由密钥流发生器 f 产生 $z_i=f(k,\sigma_i)$，这里的 σ_i 是加密器中的记忆元件(存储器)在时刻 i 的状态，f 是由密钥 k 和 σ_i 产生的函数，如图 4-2 所示。

2. 分组密码设计原理

分组密码是将明文消息编码表示后的数字(简称明文数字)序列 $x_0x_1x_2\cdots$，划分成长度为 n 的组 $x=(x_0x_1x_2\cdots x_{n-1})$(可看成长度为 n 的矢量)，每组分别在密钥 $k=(k_0k_1k_2\cdots k_{n-1})$的控制下变换成等长的输出数字(简称密文数字)序列 $y=(y_0y_1y_2\cdots y_{n-1})$，其加密函数是 $E: V_n\times K\rightarrow V_n$，$V_n$ 是 n 维矢量空间，K 为密钥空间，如图 4-1 所示。在相同的密钥 k 的控制下，加密函数可以看成是函数 $E(o,k): V_n\rightarrow V_n$。这实质上是对字长为 n 的数字序列进行置换。在二元的情况下，x 和 y 都是二元序列，共有 2^n 个不同的明文分组。为了使加密运算可逆，从而解密运算可行，每个明文分组应对应唯一的一个密文分组，即置换 $E(o,k)$是可逆的。众所周知，V_n 上这样的置换共有 $2^n!$ 个，因而密钥个数最多为 $2^n!$ 个。实际应用中的许多分组密码，如 DES、IDEA 等，所用的置换只不过是上述置换集中一个很小的子集。

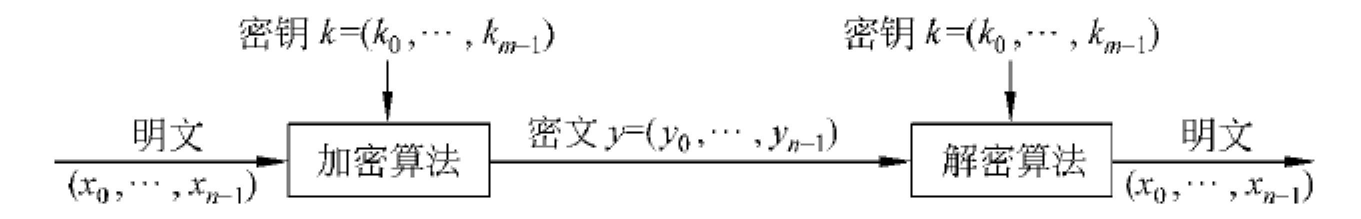


图 4-1 分组密码模型

分组密码设计就是要找到一种算法，能在密钥的控制下，从一个足够大、足够好的置换子集中简单迅速地选出一个置换，对当前输入的明文数字组进行加密变换。因此，设计的算法应满足下述安全性和软/硬件实现的要求。

- 分组长度应足够大，使得不同明文分组的个数 2^n 足够大，以防止明文被穷举法攻击。例如，若 $n=64$，则在进行攻击时用 2^{32} 个分组密文成功的概率为 1/2，同时需要 $2^{32}\times 64\text{b}=2^{15}\text{MB}$ 的存储空间，因而采取穷举法攻击是不可行的。新的算法标准一般要求 $n=128$。
- 密钥空间应足够大，尽可能消除弱密钥，从而使所有密钥同等概率，以防穷举密钥攻击。同时，密钥不能太长，以利于密钥管理。DES 采用 56 位有效密钥，现在看来显然不够长，256 位密钥应该是足够安全的。
- 由密钥确定的算法要足够复杂，充分实现明文与密钥的扩散和混淆，没有简单关系可循，要能抵抗各种已知的攻击，如差分攻击和线性攻击等；另外，还要求有较高的非线性阶数。
- 软件实现的要求。尽量使用适合编程的子块和简单的运算。密码运算在子块上进行，因此要求子块的长度能适应软件编程，如 8、16、32 位等。应尽量避免按位

置换，在子块上进行的密码运算应尽量采用易于软件实现的运算。最好是使用处理器的基本运算，如逻辑非、与、或、移位运算等。

- 硬件实现的要求。加密和解密应具有相似性，即加密和解密过程的不同应仅仅在于密钥的使用方式上，以便采用同样的器件来实现加密和解密，以节省费用和时间。尽量采用标准的组件结构，以便能在超大规模集成电路中实现。

需要指出的是，混淆和扩散是 Shannon 提出的设计密码系统的两种基本方法。Shannon 认为，在理想密码系统中，密文的所有统计特性都应与所使用的密钥独立，然而实用的密码系统都很难达到这个目标。在扩散中，要求明文的统计结构扩散消失到密文的统计特性中。要做到这一点，必须让明文的每个位影响到密文许多位的取值，即每个密文位被许多明文位影响。所有的分组密码都包含明文分组到密文分组的代换，而具体代换依赖于密钥。混淆则是试图使得密文的统计特性与密钥的取值之间的关系尽量复杂。扩散和混淆的目的都是为了挫败推测出密钥的尝试，从而抗击统计分析。

迭代密码是实现混淆和扩散原则的一种有效方法。合理选择的轮函数经过若干次迭代后能够提供必要的混淆和扩散。分组密码由加密算法、解密算法和密钥扩展算法三部分组成。解密算法是加密算法的逆过程，由加密算法唯一确定，因而主要讨论加密算法和密钥扩展算法。

3. 流密码简介

前面已经介绍了流密码的基本思想，利用密钥 k 生成一个密钥流 $z=z_0, z_1, \cdots$，密钥流由密钥流生成器 f 产生 $z_i=f(k,\sigma_i)$，这里的 σ_i 是加密器中的记忆元件(存储器)在时刻 i 的状态，f 是由密钥 k 和 σ_i 生成的函数，而 $\sigma_i(i>0)$ 可能依赖于 $k, \sigma_0, x_0, x_1, \cdots, x_{i-1}$ 等参数。

根据加密器中记忆元件的存储状态 σ_i 是否依赖于输入的明文字符，流密码可进一步分成同步和自同步两种。σ_i 独立于明文字符的叫做同步流密码，否则叫做自同步流密码。由于自同步流密码密钥流的生成与明文有关，因而较难从理论上进行分析。目前大多数研究成果都是关于同步流密码的。在这里，只介绍同步流密码。

1）同步流密码

在同步流密码中，由于 $z_i=f(k,\sigma_i)$ 与明文字符无关，因而密文字符 $y_i=e_{zi}(x_i)$ 也不依赖于此前的明文字符。因此，可将同步流密码的加密器分成密钥流生成器和加密变换器两个部分。如果与上述加密变换对应的解密变换为 $x_i=d_{zi}(x_i)$，则可给出同步流密码的模型。

一次一密码是加密流密码的原型。事实上，如果 $z_i=k_i$(即密钥用做滚动密钥流)，则加法流密码就退化成一次一密码。实际使用中，密码设计者的最大愿望是设计出一个滚动密钥生成器，使得密钥 k 经其扩展成的密钥流序列 z 具有如下一些性质。

- 极大的周期。
- 良好的统计特性。
- 抗线性分析。
- 抗统计分析。

2）密钥流生成器

同步流密码的关键技术是密钥流生成器。一般可将其看成是一个参数为 k 的有限状态自动机，由一个输出符号集 z、一个状态集 Σ、两个函数 φ 和 Ψ 及一个初始状态 σ_0 所组成，如图 4-2 所示。状态转移函数 $\varphi: \sigma_i \to \sigma_{i+1}$，将当前状态 σ_i 变为一个新状态 σ_{i+1}：输出函数 $\Psi: \sigma_i \to z_i$ 将当前状态 σ_i 变为输出符号集中的一个元素 z_i。这种密钥流生成器设计的关键在于找出适当的状态转移函数 φ 和输出函数 Ψ，使得输出序列 z 满足极大的周期、良好的统计特性、抗线性分析和抗统计分析等要求，并且要在计算设备上是节省的和容易实现的。为了实现这一目标，必须采用非线性函数。

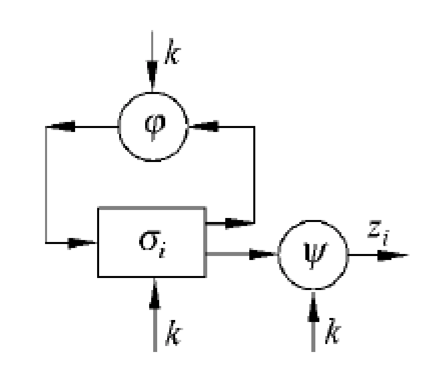


图 4-2 流密码生成器

密钥流事实上是一个无限长序列。由于一个有限状态机在确定的逻辑连接下，迟早要进入周期状态。因而实际得到的密钥流本质上是一个周期序列。用 S 表示序列 $s_0, s_1, \cdots$，如果存在正整数 p，使得 $s_i + p = s_i, i = 0, 1, 2, \cdots$，则称序列 s 为周期序列，满足上式的最小正整数 p 称为序列 s 的周期。在实际应用中，p 值越大越好。

4.1.5 DES 算法

数据加密标准 DES(Data Encryption Standard)是迄今为止使用最为广泛的经典加密算法。1973 年 5 月 13 日美国国家标准局 NBS(National Bureau of Standards)公布了一项公告，征求国家密码标准方案。IBM 提交了他们研制的一种密码算法，该算法是由早期的 LUCIFER 密码改进而得的。在经过大量的公开讨论之后该密码算法于 1977 年 1 月 15 日被正式批准为美国联邦信息处理标准，即 FIPS-46，同年 7 月 15 日生效。并规定每隔 5 年由美国国家保密局(National Security Agency)重新评估它是否继续作为联邦加密标准。最近的一次评估是在 1994 年 1 月，当时决定在 1998 年 12 月以后，DES 不再作为联邦加密标准。新的美国联邦加密标准称为高级加密标准 AES(Advanced Encryption Standard)。尽管如此，DES 对推进密码理论的发展和应用仍起了重要作用，并对学习和研究分组密码的基本理论、设计思想和实际应用有着珍贵的参考价值。DES 是分组长度为 64 位的分组密码算法，密钥长度也是 64 位，其中每 8 位有一位奇偶校验位，因此有效密钥长度为 56 位。DES 算法是公开的，其安全性依赖于密钥的保密程度。DES 结构框图如图 4-3 所示。

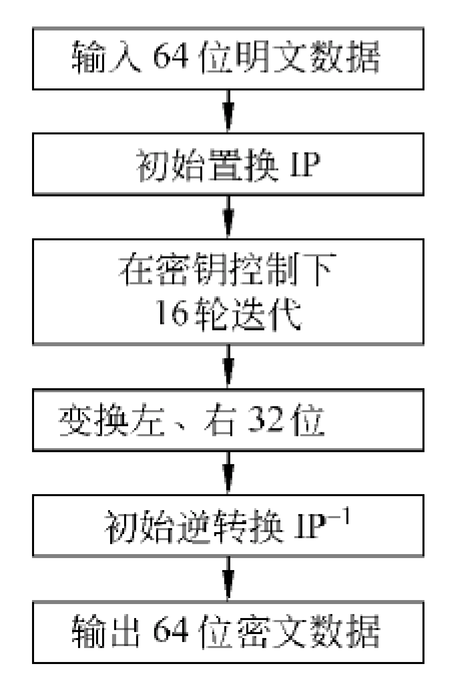


图 4-3 DES 算法结构图

1. 初始置换 IP 和初始逆置换 IP^{-1}

将 64 位明文数据用初始置换 P 置换，得到一个乱序的 64 位明文分组，然后分成左、右等长的 32 位，分别记为 L_0 和 R_0。进行 16 轮完全类似的迭代运算后，将所得左、右长度相等的两半 L_{16} 和 R_{16} 交换得到 64 位数据 $R_{16}L_{16}$，最后再用初始逆置换 IP^{-1} 进行置换，产生密文数据组。置换表自左向右、自上而下的 64 个位置对应 64 位数据组，置换表中的数字表示将 64 位数据组中该数字所在位置的位

置换为该数字表示的位置的位。初始置换 IP 和初始逆置换 IP^{-1} 如表 4-3 所示。

表 4-3　初始转换与初始逆置换

初始置换 IP								初始逆置换 IP^{-1}							
58	50	42	34	26	18	10	2	40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6	38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	51	19	59	27
61	53	45	37	29	21	13	5	34	2	42	10	50	18	58	26
63	55	47	39	31	23	15	7	33	1	41	9	49	17	57	25

初始置换 IP 的含义是：

58 是指将原第 58 位数码换位到当前位置，即第 1 位。

50 是指将原第 50 位数码换位到当前位置，即第 2 位。

42 是指将原第 42 位数码换位到当前位置，即第 3 位。

……

7 是指将原第 7 位数码换位到当前位置，即第 64 位。

2. 迭代变换

迭代变换是 DES 算法的核心部分，如图 4-4 和图 4-5 所示。每一轮开始时将输入的

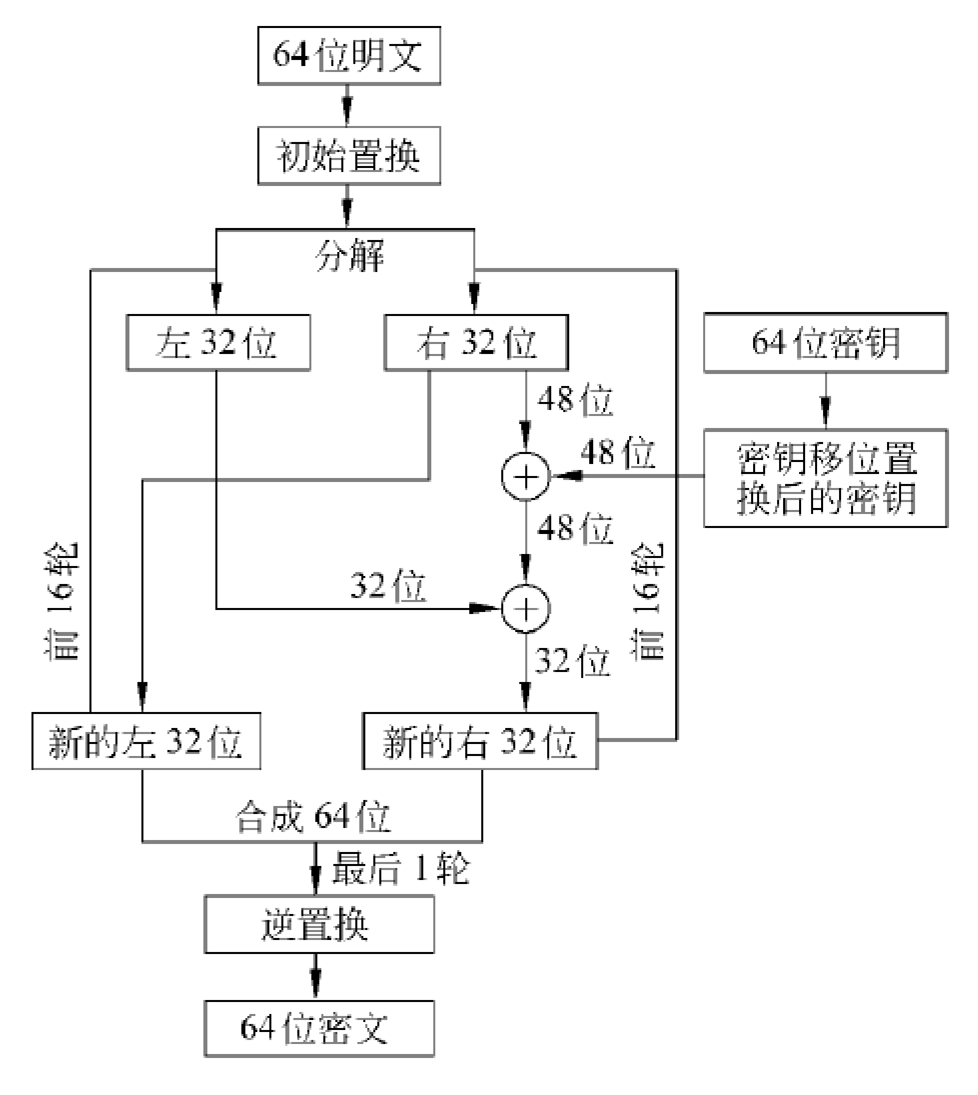


图 4-4　DES 算法流程

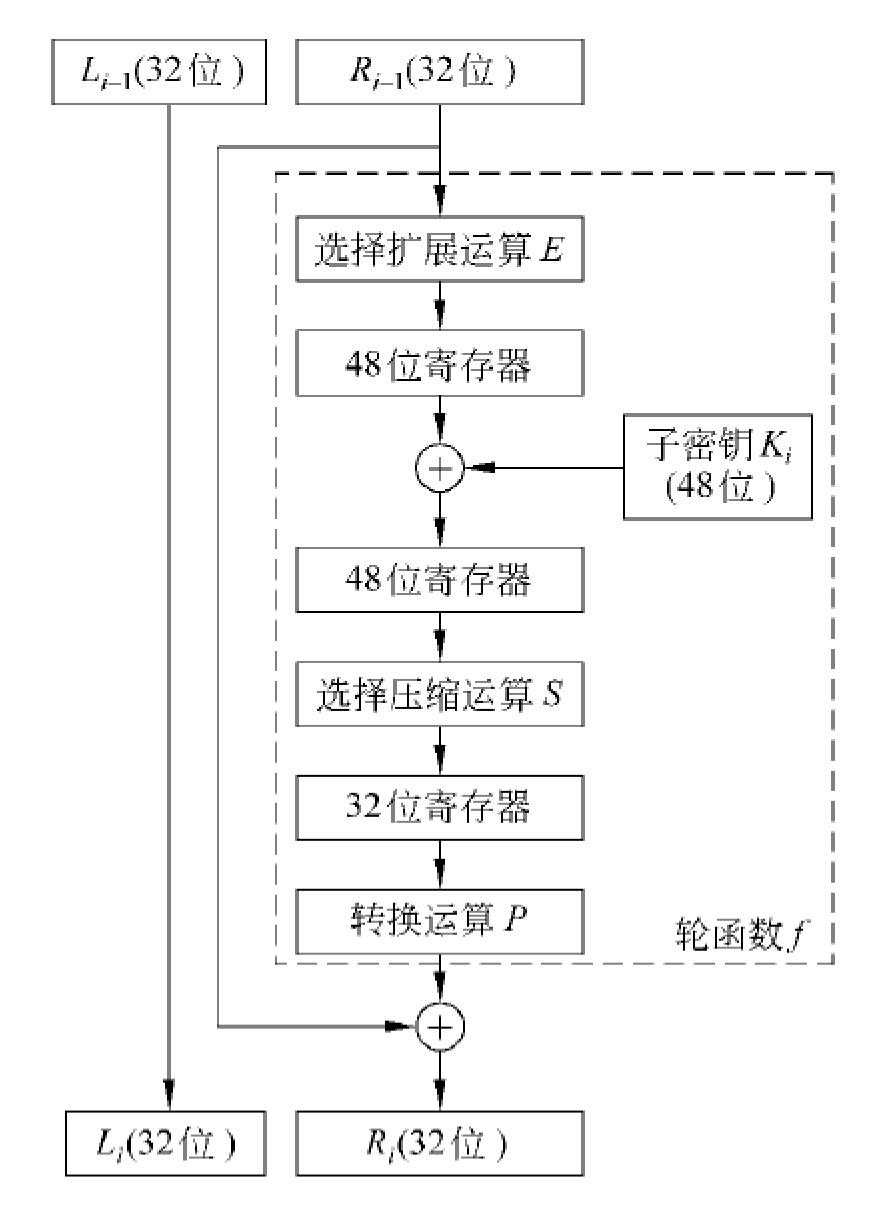


图 4-5 DES 迭代过程

64 位数码分成左右相等的两半,右半部分原封不动地作为本一轮输出的 64 位数据的左半部分,同时对右半部分进行一系列的变换,即用轮函数 F 作用于右半部分,然后将得结果(32 位数据)与输入数据的左半部分进行逐位异或,最后将所得结果作为本轮输出的 64 位数据的右半部分。

从图 4-5 可以看出,轮函数 F 由选择扩展运算 E、与子密钥的异或运算、选择压缩运算 S 和转换运算 P 组成。

3. 选择扩展运算 *E*

将输入的 32 位数据扩展为 48 位的输出数据,其实施的变换运算如表 4-4 所示。

表 4-4 选择扩展运算 *E*

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

表中的第 1、2 两列实际上是第 5、6 两列的变换。

如果将输入的 32 位数据按表 E 中所标位置顺序读出，则可得到 48 位的输出数据。

4. 与子密钥的异或运算

将选择扩展运算的 48 位输出数据与子密钥 K_i(48 位)进行异或运算。

5. 选择压缩运算(S 盒置换)

将输入的 48 位数据从左到右分成 8 组，每一组 6 位。然后输入到 8 个 S 盒中，每个 S 盒均为非线性代换，输出为 4 位，如图 4-6 所示。

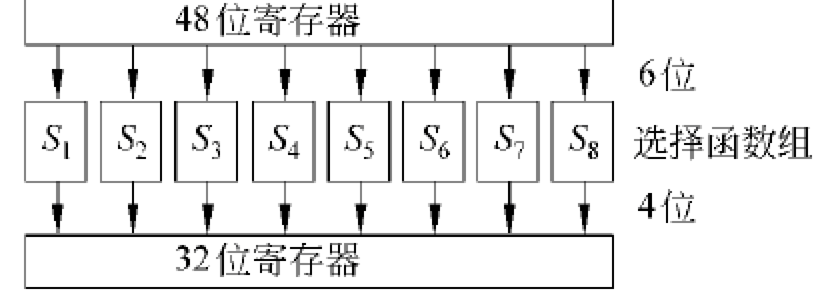


图 4-6 选择压缩运算

对于每一个 S_i，6 位输入中的第 1 和第 6 位组成的二进制数用来确定 S 盒(如表 4-5 所示)中的行，中间 4 位(第 2～5 位)用来确定 S 盒中的列。将 S_i 中相应的行、列位置的十进制数转换成 4 位二进制数表示作为输出(即输入 6 位输出 4 位)。

表 4-5 S 盒运算表

	行/列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

续表

	行/列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	1	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

例 4-4　S_2的输入为 101001，则行数和列数的二进制表示分别是 11(第 1 位和第 6 位)和 0100(中间 4 位)，即第 3 行和第 4 列，查 S 盒可知，S_2 的第 3 行第 4 列的十进制数为 3，用 4 位二进制数表示为 0011，所以 S_2 的输出为 0011。

例 4-5　设 S_3 的输入为 110101，则有：

$$b_1 b_6 = (11)_2 = 3 \qquad b_2 b_3 b_4 b_5 = (1010)_2 = 10$$

$$S_3(3,10) = (14)_{10} = (1110)_2$$

即 S_3 输出为 1110。

6. 置换 *P*

置换 P 如表 4-6 所示。

表 4-6　*P* 置换表

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

最后需要描述的是用密钥 K 来产生 16 个 48 位的子密钥 K_i，$1 \leqslant i \leqslant 16$。

7. 子密钥的产生

给定 64 位的密钥 K，用置换选择 1(PC－1)进行置换，去掉了输入的第 8、16、24、32、40、48、56、64 位(因这 8 位通常是奇偶校验位)，并重排实际 56 位的密钥。将得到的 56 位数据分成左、右等长的 28 位，分别记为 C_0 和 D_0。对 $1 \leqslant i \leqslant 16$，计算 $C_i = LS_i(C_{i-1})$ 和 $D_i = LS_i(D_{i-1})$。将每轮 56 位数据 C_iD_i 用置换选择 2(PC－2)作用，去掉第 9、18、22、25、35、38、43、54 位，同时重排剩下的 48 位，输出作为 K_i，产生子密钥的密钥编排算法如图 4-7 所示。这里 LS_i 表示循环左移 1 位(当 $i=1,2,9,16$ 时)或 2 位(其他情况)，如表 4-7 所示。置换选择 1(PC－1)和置换选择 2(PC－2)如表 4-8 所示。

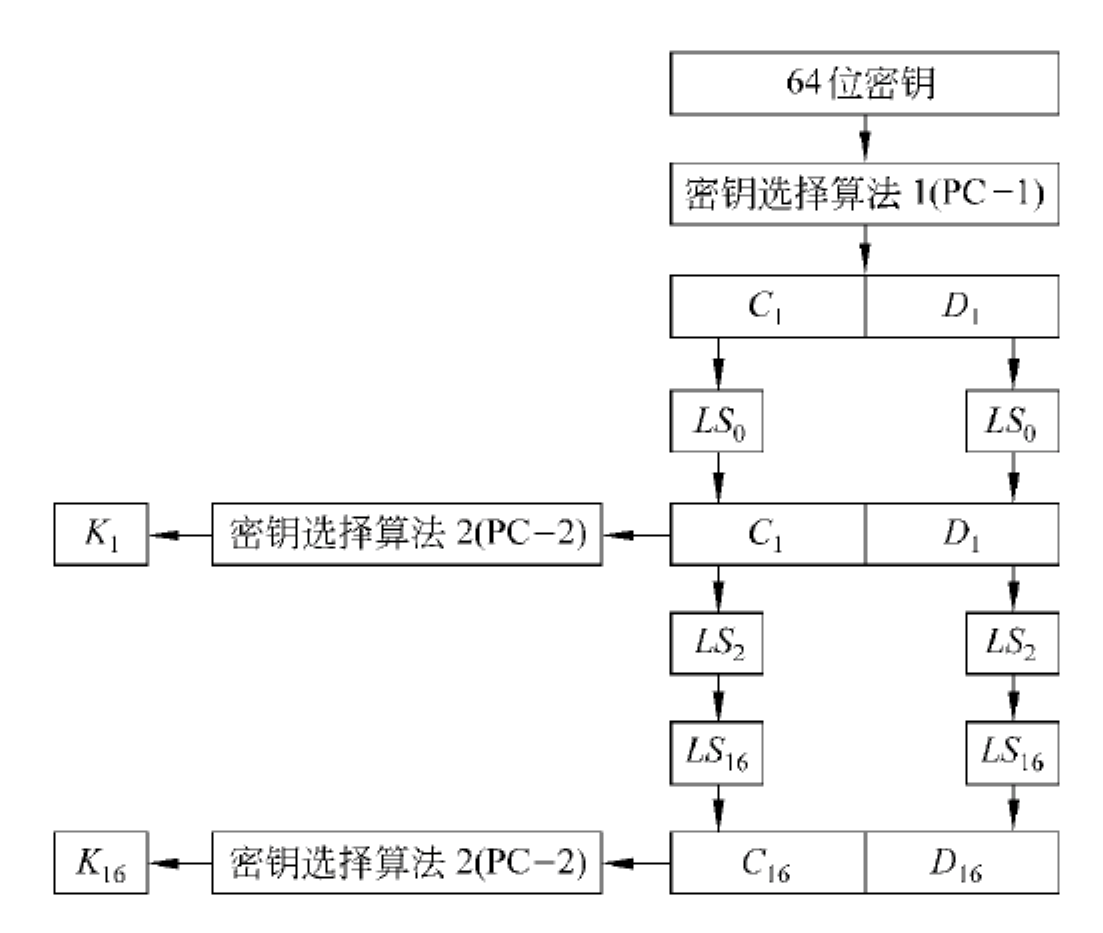


图 4-7 子密钥编排算法流程

表 4-7 循环移位表

轮数	LS_1	LS_2	LS_3	LS_4	LS_5	LS_6	LS_7	LS_8
位数	1	1	2	2	2	2	2	2
轮数	LS_9	LS_{10}	LS_{11}	LS_{12}	LS_{13}	LS_{14}	LS_{15}	LS_{16}
位数	1	2	2	2	2	2	2	1

进行 16 轮完全相同的迭代运算后，将所得左、右长度相等的两半 L_{16} 和 R_{16} 交换，得出 64 位数据 R_{16} 和 L_{16}，用初始逆转换 IP^{-1} 进行转换，产生密文数据组，转换表自左至右、自上而下的 64 个位置对应 64 位数据组，置换表中的数字表示将 64 位数据组中该数字所在位置的位置换为该数字表示的位置的位。

8. 解密

由于 DES 算法是在 Feistel 网络结构的输入和输出阶段分别添加初始置换 IP 和初

始逆置换 IP^{-1}而构成的，所以它的解密使用与加密同样的算法，只是子密钥的使用次序相反。

表 4-8 PC—1 置换与 PC—2 置换

PC—1							PC—2					
57	49	41	33	25	17	9	14	17	11	24	1	5
1	58	50	42	34	26	18	3	28	15	6	21	10
10	2	59	51	43	35	27	23	19	12	4	26	8
19	11	3	60	52	44	36	16	7	27	20	13	2
63	55	47	39	31	23	15	41	52	31	37	47	55
7	62	54	46	38	30	22	30	40	51	45	33	48
14	6	61	53	45	37	29	44	49	39	56	34	53
21	13	5	28	20	12	4	46	42	50	36	29	32

4.1.6 消息摘要

1. 消息摘要

消息摘要又称报文摘要，其基本思想如下：

通常来说，报文的加密可通过 DES 加密技术、AES 加密技术来实现，而报文的鉴别则可通过数字凭证技术进行加密和认证。

但在特定的网络环境中，许多报文并不需要加密，但是要求发送的报文应该是完整的和不可伪造的。例如，通过网络通知网络上所有用户有关上网的注意事项。对于不需要加密的报文进行加密和解密，将给计算机增加很多不必要的开销，因此，可使用报文摘要 MD 算法来进行报文鉴别算法来达到目的。

报文摘要算法过程如下：

- 发送方将待发送的可变长的报文 m 经过 MD 算法计算得出固定长度(如 128 位)的报文摘要 H(m)。
- 对 H(m)加密生成密文 E_k(H(m))附加在报文 m 之后传送给接收方，如图 4-8(a)所示。
- 在接收端收到报文 m 和报文摘要 E_k(H(m))密文之后，将报文摘要密文E_k(H(m))解密还原成 H(m)。
- 同时在接收端将收到的报文 m 经过 MD 算法运算得出的报文摘要 H(m′)与 H(m) 比较是否相同，若不相同则可断定收到的报文在传输过程中已被篡改。其解密过程如图 4-8(b)所示。

报文摘要的优点是对于一个有限长度报文摘要 H(m)进行加密比对整个报文 m 进行加密效率要高得多，但对鉴别报文 m 来说，其效果是一样的。也就是说 m 和E_k(H(m))

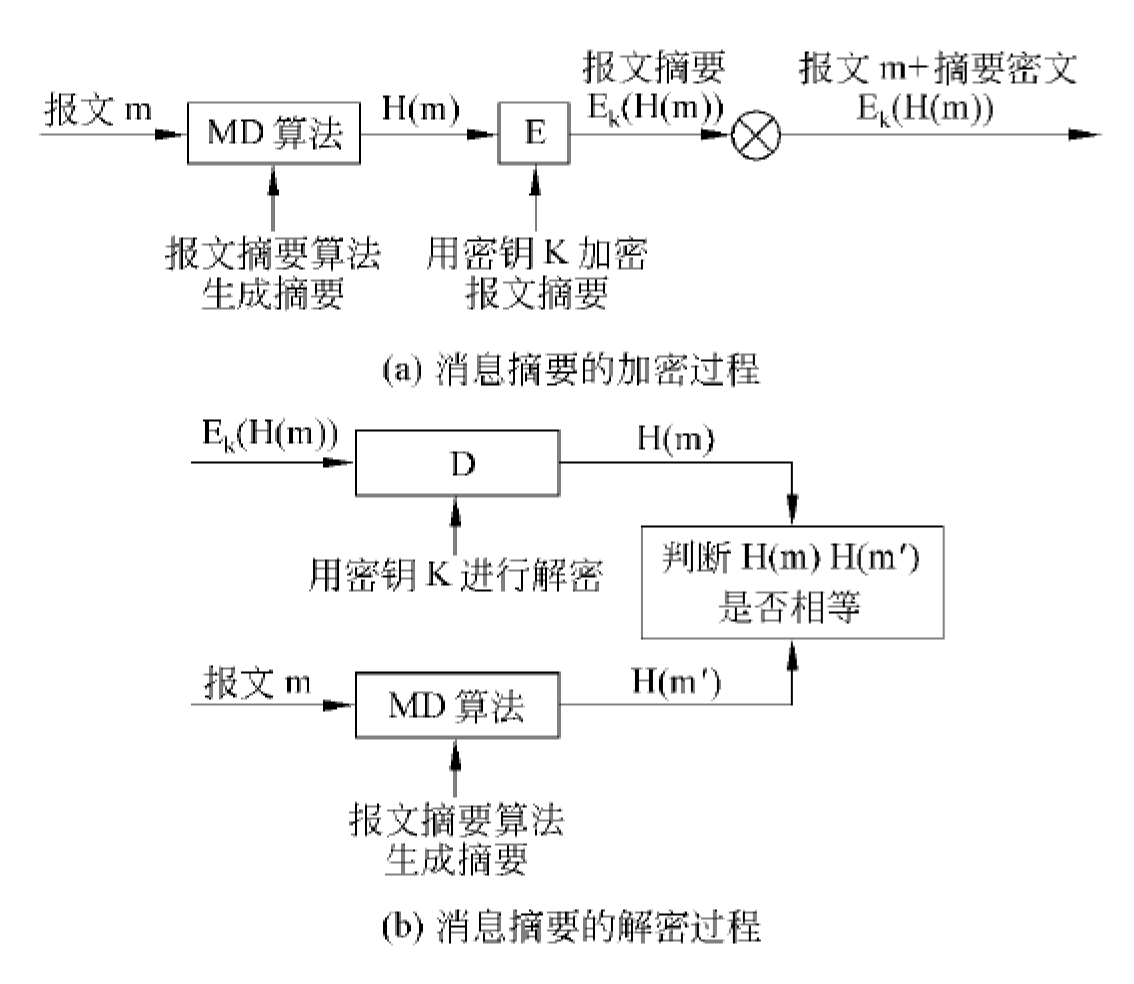


图 4-8 消息摘要的加密和解密过程

在一起是不可篡改和不可伪造的，是可鉴别和不可抵赖的。

2. MD5 算法

MD5 算法以 512 位(64 字节)分组来处理输入的消息，每个分组又划分为 16 个 32 位的子分组(32×16＝512)。算法的输出是 4 个 32 位分组，将它们级联起来得到一个 128 位(32×4＝128)的散列值。

MD5 算法的处理过程如下：

1）消息填充

要求整个消息必须是 512 位的整数倍，如果不满足，则要进行填充。其填充方法是，在消息后面先填充一个 1，然后是若干个 0，最后是一个 64 位的实际长度值，如下所示。

消息	10000000…00	消息长度(64 位)

2）变量初始化

初始化 4 个 32 位变量 A、B、C、D(链接变量)，用十六进制表示，初始值为：

A＝01234567；B＝89abcdef；C＝fedcba98；D＝76543210

3）算法主循环

循环次数是消息中 512 位分组的数目。首先把 4 个链接变量复制到另一组变量中：

a←A；　b←B；　c←C；　d←D

然后进入主循环，主循环有 4 轮，每一轮基本相似，共 16 次操作。每次操作对 a，b，c 和 d 中的 3 个变量进行一次非线性函数运算，然后将所得结果与第 4 个变量、一个子分组和一个常数相加，再将所得结果向左循环移位若干位，并与 a、b、c 和 d 中的一个相加。最后用该结果取代 a、b、c 和 d 之一。

每一轮循环中，使用一个非线性函数，4 轮共使用了 4 个非线性函数。它们分别是：

$$F(X,Y,Z)=(X\wedge Y)\vee((\neg X)\wedge Z)$$

$$G(X,Y,Z)=(X\wedge Z)\vee(Y\wedge(\neg Z))$$

$$H(X,Y,Z)=X\oplus Y\oplus Z$$

$$I(X,Y,Z)=Y\oplus(X\vee(\neg Z))$$

其中“⊕”为“异或”运算，“∧”为“与”运算，“∨”为“或”运算，“¬”为“求反”运算（“非”运算）。

设 M_j 为消息的第 j 个子分组（j 的取值范围是 0～15），L_s 表示循环左移 s 位，则上述 4 种操作分别为：

FF(a,b,c,d,M_j,s,t_i)表示 a=b+((a+F(b,c,d)+M_j+t_i)L_s

GG(a,b,c,d,M_j,s,t_i)表示 a=b+((a+G(b,c,d)+M_j+t_i)L_s

HH(a,b,c,d,M_j,s,t_i)表示 a=b+((a+H(b,c,d)+M_j+t_i)L_s

II(a,b,c,d,M_j,s,t_i)表示 a=b+((a+I(b,c,d)+M_j+t_i)L_s

第一轮运算为：

FF(a,b,c,d,M_0,7,d76aa478)，　FF(d,a,b,c,M_1,12,e8c7b756)
FF(c,d,a,b,M_2,17,242070db)，　FF(b,c,d,a,M_3,22,c1bdceee)
FF(a,b,c,d,M_4,7,f57c0faf)，　FF(d,a,b,c,M_5,12,4787c62a)
FF(c,d,a,b,M_6,17,a8304613)，　FF(b,c,d,a,M_7,22,fd469501)
FF(a,b,c,d,M_8,7,698098d8)，　FF(d,a,b,c,M_9,12,8b44f7af)
FF(c,d,a,b,M_{10},17,ffff5bb1)，　FF(b,c,d,a,M_{11},22,895cd7be)
FF(a,b,c,d,M_{12},7,6b901122)，　FF(d,a,b,c,M_{13},12,fd987193)
FF(c,d,a,b,M_{14},17,a679438e)，　FF(b,c,d,a,M_{15},22,49b40821)

第二轮运算为：

GG(a,b,c,d,M_1,5,f61e2562)，　GG(d,a,b,c,M_6,9,c040b340)
GG(c,d,a,b,M_{11},14,265e5a51)，　GG(b,c,d,a,M_0,20,e9b6c7aa)
GG(a,b,c,d,M_5,5,d62f105d)，　GG(d,a,b,c,M_{10},9,02441453)
GG(c,d,a,b,M_{15},14,d8a1e681)，　GG(b,c,d,a,M_4,20,e7d3fbc8)
GG(a,b,c,d,M_9,5,21e1cde6)，　GG(d,a,b,c,M_{14},9, c33707d6)
GG(c,d,a,b,M_3,14,f4d50d87)，　GG(b,c,d,a,M_8,20,455a14ed)
GG(a,b,c,d,M_{13},5,a9e3e905)，　GG(d,a,b,c,M_2,9, fcefa3f8)
GG(c,d,a,b,M_7,14,676f02d9)，　GG(b,c,d,a,M_{12},20,8d2a4c8a)

第三轮运算为：

HH(a,b,c,d,M_5,4,fffa3942)，　HH(d,a,b,c,M_8,11,8771f681)
HH(c,d,a,b,M_{11},16,6d9d6122)，　HH(b,c,d,a,M_{14},23,fde5380c)
HH(a,b,c,d,M_1,4,a4beea44)，　HH(d,a,b,c,M_4,11,4bdecfa9)
HH(c,d,a,b,M_7,16,f6bb4b60)，　HH(b,c,d,a,M_{10},23,bebfbc70)
HH(a,b,c,d,M_{13},4,289b7ec6)，　HH(d,a,b,c,M_0,11, xeaa127a)
HH(c,d,a,b,M_3,16,d4ef3085)，　HH(b,c,d,a,M_6,23,04881d05)

HH(a,b,c,d,M_9,4,d9d4d039), HH(d,a,b,c,M_{12},11,e6db99e5)
HH(c,d,a,b,M_{15},16,1fa27cf8), HH(b,c,d,a,M_2,23,c4ac5665)

第四轮运算为:

II(a,b,c,d,M_0,6,f4292244), II(d,a,b,c,M_7,10, 432aff97)
II(c,d,a,b,M_{14},15,ab9423a7), II(b,c,d,a,M_5,21,fc93a039)
II(a,b,c,d,M_{12},6,655b58c3), II(d,a,b,c,M_3,10, 8f0ccc92)
II(c,d,a,b,M_{10},15,ffeff47d), II(b,c,d,a,M_1,21,85845dd1)
II(a,b,c,d,M_8,6,6fa87e4f), II(d,a,b,c,M_{15},10, fe2ce6e0)
II(c,d,a,b,M_6,15,a3014314), II(b,c,d,a,M_{13},21,4e0811a1)
II(a,b,c,d,M_4,6,f7537e82), II(d,a,b,c,M_{11},10, bd3af235)
II(c,d,a,b,M_2,15,2ad7d2bb), II(b,c,d,a,M_9,21,eb86d391)

在所有运算完成后,将 A、B、C、D 分别加上 a、b、c、d 的值。然后使用下一个分组数据继续进行上述运算。

4) 输出结果

将最后输出的 A、B、C、D 的值级联起来,形成一个 128 位散列值,也就是 MD5 算法的消息摘要值。

4.1.7 公开密钥加密体制

前面介绍的对称密码体制的一个显著的缺点是,在进行保密通信时,发送者与接收者需要使用一个安全的通信信道来建立会话密钥,即要通过一个安全的信道来传送密码。这可以通过两种方式解决,其一,若信源方已制定了一个密码(共享密钥),可通过对该密钥进行加密后传输给信宿方;其二,通信双方都通过密钥分配中心申请获取一个会话密钥。前者可以用人工方式传递共享密钥;后者需要通信双方都与密钥分配中心有一个共享密钥,共享密钥同样用人工等方式传递。因而密钥分配成本很高,并且依赖于信使或密钥分配中心的可靠性。在某些情况下,甚至无法及时获得建立会话密钥所需的合理安全信道。因此,通信双方也就不能进行信息的安全传输。为解决这一问题,引入了公开密钥加密体制。

1. 公开密钥加密算法的特点

在公开密钥密码体制中,使用一个加密算法 E 和一个解密算法 D,E 和 D 是不相同的,E 是公开的(这就是“公开密钥”一词的出处),一般的用户(通常指第三方非法攻击者)即使知道了 E,也是无法推导出 D 的。

公开密钥体制有 3 个特点:

- D(E(P))=P。
- 由 E 来推断 D 是极其困难的。
- 用已选定的明文进行分析,是不能破译 E 的。

只要满足了上述 3 个条件,则加密算法 E 是可以公开的。公开密钥密码体制如图 4-9 所示。

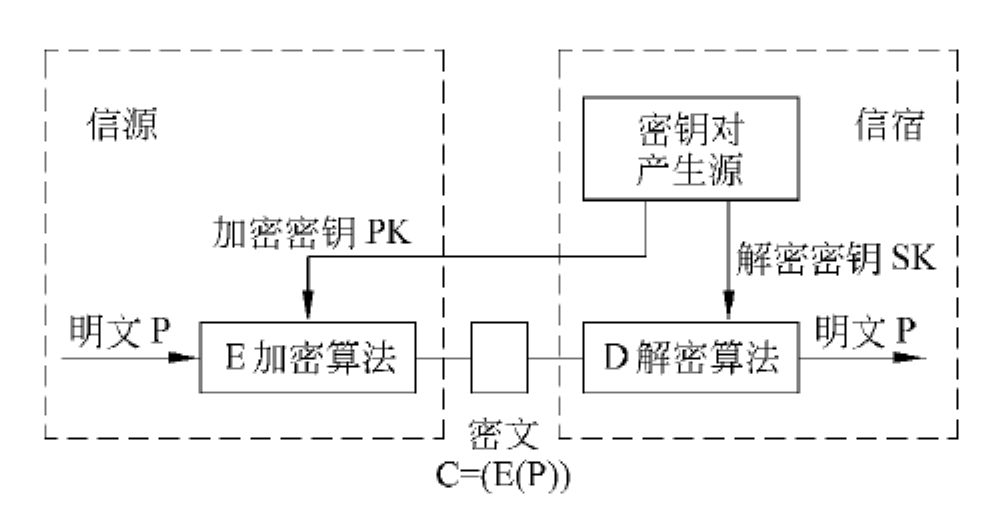


图 4-9 公开密钥加密体制的加密流程

2. 如何用公开密钥进行加、解密

现在考虑两个用户 A 和 B,两者从未联系过,而要想在 A 和 B 之间建立保密信道。A 所确定的加密密钥为 E_A,B 的加密密钥为 E_B,并将 E_A 和 E_B 放在网上作为公共可读文件(共享文件)内。现在 A 要发送报文 P 给 B,首先算出密文 $C=E_B(P)$,即用 B 方的公开密钥进行加密,并把他发送给 B。B 收到密文 $C= E_B(P)$后,使用密钥 D_B 进行解密,即

$$D_B(E_B(P))=P$$

在这里,E_B 是公开的而 D_B 是不公开的,从而达到保密的目的。因为解密算法 D_B 只有 B 才知道,所以只有 B 才能对密文 $E_B(P)$进行解密。其加密/解密过程如图 4-9 所示。

在介绍公开密钥算法之前,先介绍一个术语"单向函数",如果对一个函数 f 的定义域上的任意一个 x 容易计算出 $f(x)$的值,但对 f 的值域上的任意一个 y,$f^{-1}(y)$在计算上不可行,就称 f 是单向函数。

单向函数是密码学中的一项重要的研究内容,在现实中,确实存在许多函数被认为是单向的(即具有单向函数的)。这里给出一个可信程度很高的单向函数的例子。

假设 n 是两个大素数 p 和 q 的乘积,分解 n 被认为是一个非常困难的问题。并设 b 是一个正整数,定义函数 f: $Z_n \to Z_n$,$f(x)=x^b \bmod n$,则 f 被认为是一个单向函数。当知道了 n 的因子是 p 或 q 时,计算逆是容易的,因而 f 是陷门单向函数。

在这里,介绍的是 RSA 公开密钥加密体制,该算法是由 R. Rivest、A. Shamir 和 L. Adleman 3 个人在 1977 年共同提出的,称为 RSA(RSA 是取这 3 位研制者姓的首字母的组合)算法。

3. RSA 算法描述

RSA 算法正是利用了陷门单向函数的一种可逆模指数运算。它的安全性是基于大整数分解因子的困难性的理论基础。

1) RSA 密码体制的建立

建立一个 RSA 密码体制的过程如下:

- 选择两个大素数 p 和 q。
- 计算乘积 $n=pq$ 和 $\varphi(n)=(p-1)(q-1)$。
- 选择一个大于 1 而小于 $\varphi(n)$的随机整数 e,使得 $\gcd(e, \varphi(n))=1$ (这里的 gcd()

为互质函数)。

- 计算 d 使得 $de=1 \bmod \varphi(n)$,即 $de \bmod \varphi(n)=1$
- 对每一个密钥 $k=(n,p,q,d,e)$,定义加密变换为 $y=E_k(x)=x^e \bmod n$,解密变换为 $D_k(x)=y^d \bmod n$,这里 $x,y\in Z_n$。
- 将$\{e,n\}$作为公开密钥,$\{d,n\}$作为私有密钥。

这样就建立了一个明文空间 P 和密文空间 C 为 $P=C=Z_n$,密钥空间为 $K=\{(n,p,q,e,d): n=pq, p$ 和 q 是大素数,$1<e,d<\varphi(n): de=1 \bmod \varphi(n)\}$的 RSA 密码体制。

设接收方 B 在网上公开他的公钥,并希望向他发送一个消息 P,发送方 A 计算密文 $C=P^e \bmod n$,并将 C 传送给 B,B 收到密文 C 后通过计算 $P=C^d \bmod n$ 进行解密。

由于这里选择的 e 和 d 满足 $ed=1 \bmod \varphi(n)$,因而 ed 具有 $k\varphi(n)+1$ 的形式。

2) RSA 算法实例

例 4-6 用两个小素数 7 和 17 来建立一个简单的 RSA 算法。

① 选择两个素数 $p=7$ 和 $q=17$。

② 计算得 $n=p\times q=7\times 17=119$,$\varphi(n)=(p-1)\times(q-1)=6\times 16=96$。

③ 选择一个随机整数 $e=5$,$e>1$ 且小于 $\varphi(n)$并且与 $\varphi(n)$互质。

④ 求出 d,使得 $de=1 \bmod 96$ 且 $d<96$,此处求出 $d=77$,因为 $77\times 5=385=4\times 96+1$。

⑤ 设 $P=19$,计算 19 模 119 的 5 次幂,$P^e=19^5 \bmod 119=66$,即密文 $C=66$。

⑥ 接收方收到密文 66 后,计算 66 模 119 的 77 次幂:$P=C^d=66^{77} \bmod 119$ 得到明文 19。

当然,在实际应用中 p、q、n、e 和 d 都要取很大的值,通常 p 和 q 的值应是 100 位以上的十进制整数。

4.2 访问控制技术与安全审计技术

4.2.1 访问控制技术

访问控制是一门研究用户对资源的访问权限进行控制的技术。访问控制策略基于两点:

- 有效地保障合法用户(授权用户)访问资源。
- 拒绝非法用户(非授权用户)访问资源。

1. 访问控制目标

在用户身份认证和授权之后,访问控制机制将根据预先设定的规则对用户访问某项资源(目标)进行控制,只有规则允许时才能访问,违反预定安全规则的访问行为将被拒绝。资源可以是信息资源、处理资源、通信资源或者物理资源,访问方式可以是获取信息、修改信息或者完成某种功能,一般情况可以理解为读、写或者执行的访问行为。

访问控制的目的是为了限制访问主体对访问客体的访问权限,从而将计算机及网络系统限制在合法范围内使用。其中主体可以是某个用户,也可以是用户启动的进程和服

务。为达到此目的，访问控制需要完成以下两个任务。

- 识别和确认访问系统的用户。
- 决定该用户可以对某一系统资源进行何种类型的访问。

访问控制一般包括3种类型，自主访问控制、强制访问控制和基于角色的访问控制。下面将分别进行介绍。

2. 自主访问控制

自主访问控制DAC(Discretionary Access Control)是一种最基本的访问控制方式，它是基于对主体或主体所属的主体组的识别来限制对客体的访问，这种控制是自主的。自主是指主体能够自主地将访问权或访问权的某个子集授予其他主体。简单来说，自主访问控制就是由拥有资源的用户自己来决定一个或多个主体可以在什么程度上访问哪些资源。

自主访问控制是一种比较宽松的访问控制，一个主体的访问权限具有传递性。比如大多数交互系统的工作流程是这样的，用户首先登录，然后启动某个进程为该用户做某项工作，这个进程就继承了该用户的属性，包括访问权限。这种权限的传递可能会给系统带来安全隐患，某个主体通过继承其他主体的权限而得到了它本身不应具有的访问权限，就可能破坏系统的安全性，这是自主访问控制方式最大的缺陷。

3. 访问控制表

访问控制表ACL(Access Control List)是基于访问控制矩阵中列的自主访问控制。它在一个客体上附加一个主体明细表，用以表示各个主体对该客体的访问权限。明细表中的每一项都包括主体的身份和主体对这个客体的访问权限。如果使用组(group)或者通配符的概念，可以有效地缩短表的长度。

访问控制表是实现自主访问控制比较好的方式，下面通过例子进行详细说明。

对系统中一个需要保护的客体。O_j附加的访问控制表的结构如图4-10所示。

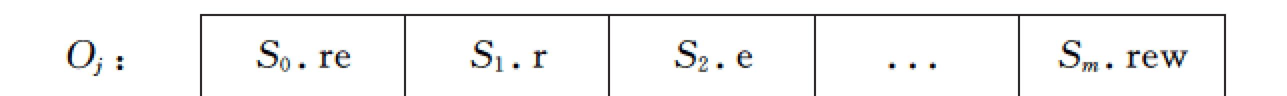


图4-10 访问控制表

其中：$S_i(i=1,2,\cdots,m)$：主体名；

r(read)：读；

e(execute)：执行；

w(write)：写；

n(no)：未授权。

在图4-10的例子中，对于客体O_j，主体S_0具有读(r)和执行(e)的权利：主体S_1只有读的权利；主体S_2只有执行的权利；而主体S_m具有读、写和执行的权利。

在一个很大的系统中，会有非常多的主体和客体，这会导致访问控制表非常长，占用

很多的存储空间，而且访问时效率下降。为解决这一问题就需要分组和使用通配符。

在多用户系统中，用户可根据部门结构或工作性质被分为几个类，同一个类中的所有用户使用的资源基本上是相同的。因此，可以把同一个类的用户作为一个组，分配一个组名，简称 GN。这时，访问控制表中的主体标识为（在这里，通配符“ * ”可以代替任何组名或者主体标识符）：

主体标识＝ID. GN

其中，ID 是主体标识符，GN 是主体所在组的组名，如图 4-11 所示。

O_j：	Liu. INFO. rew	* . INFO. re	Zhang. * . r	* . * . n

图 4-11　带有组和通配符的访问控制表

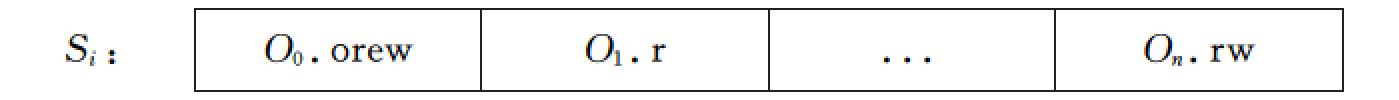
在图 4-11 的访问控制表中，第 1 个和第 2 个表项说明属于 INFO 组的所有主体都对客体 O_j 具有“读”和“执行”的权利，但只有 INFO 组中的主体 liu 才额外具有“写”的权限；第 3 个表项说明无论是哪一组中的 zhang 都可以“读”客体 O_j；最后一个表项说明所有其他的主体，无论属于哪个组，都不具备对 O_j 有任何访问权限。

在访问控制表中还需要考虑的一个问题是默认问题。默认功能的设置可以方便用户的使用，同时也避免了许多文件泄露的可能。最基本的，当一个主体生成一个客体时，该客体的访问控制表中对应生成者的表项应该设置成默认值，比如具有读、写和执行权限。另外，当某一个新的主体第一次进入系统时，应该说明它在访问控制表中的默认值，比如只有读的权限。

4. 访问能力表

前面说过，访问控制表是基于“列”的自主访问控制，而访问能力表（access capabilities list）则是基于“行”的自主访问控制。能力（capability）是为主体提供的、对客体具有特定访问权限且不可伪造的标志，它决定主体是否可以访问客体以及以什么对客体有什么访问权限。主体可以将能力转移给为自己工作的进程，在进程运行期间，还可以添加或者修改能力。能力的转移不受任何策略的限制，所以对于一个特定的客体，还不能确定所有有权访问它的主体。因此，访问能力表不能实现完备的自主访问控制，而访问控制表是可以实现的。利用访问能力表实现的自主访问控制系统不是很多，其中只有少数系统试图通过增加其他措施实现完备的自主访问控制。

图 4-12 说明了访问能力表的样式。



S_i：	O_0. orew	O_1. r	…	O_n. rw

图 4-12　访问控制能力表

图 4-12 是主体 S_i 的访问能力表，图中的每一表项包括客体的标识和 S_i 对该客体的访问能力。如图 4-12 所示，S_i 是客体 O_0 的拥有者，并对它具有最大的访问能力（读、写、执行）；S_i 对客体 O_1 只有读的能力；S_i 对客体 O_n 具有读和写的能力。

能力机制的最大特点是能力的拥有者可以在主体中转移能力。在转移的能力中有一种叫做“转移能力”，它允许接受能力的主体继续转移能力。比如，进程 A 将某个能力的备份转移给进程 B，B 又将能力的备份传递给进程 C。如果 B 不想让 C 继续转移这个能力，就在转移给 C 的能力备份中去掉转移能力，这样 C 就不能转移能力了。主体为了在能力取消时从所有主体中彻底清除自己的能力，需要跟踪所有的转移。

5. 强制访问控制

自主访问控制的最大特点是自主，即资源的拥有者对资源的访问策略具有决策权，因此是一种限制比较弱的访问控制策略。这种方式给用户带来灵活性的同时，也带来了安全隐患。

在一些系统中，需要更加强硬的控制手段，强制访问控制 MAC（Mandatory Access Control）就是一种这样的机制。

强制访问控制系统为所有的主体和客体指定安全级别，比如绝密级、机密级、秘密级和无密级。不同级别标记了不同重要程度和能力的实体。不同级别的主体对不同级别的客体的访问是在强制的安全策略下实现的。

在强制访问控制机制中，将安全级别进行排序，比如按照从高到低排列，规定高级别可在以单向访问低级别，也可以规定低级别可以单向访问高级别。这种访问可以是读，也可以是写或修改。在 Bell Lapadula 模型中，信息的完整性和保密性是分别考虑的，因而对读写的方向进行了反向规定，如图 4-13 所示。

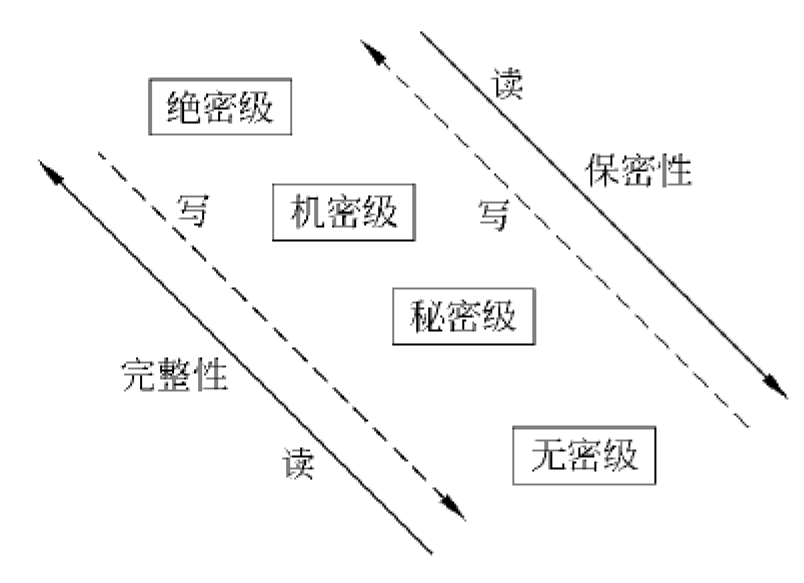


图 4-13 强制访问控制 MAC 模型

1）保障信息完整性策略

为了保障信息的完整性，低级别的主体可以读高级别客体的信息（不具保密性），但低级别的主体不能写高级别的客体（保障信息完整），因此采用的是上读/下写策略。即属于某一个安全级的主体可以读本级和本级以上的客体，可以写本级和本级以下的客体。比如机密级主体可以读绝密级、机密级的客体，可以写机密级、秘密级、无密级的客体。这样，低密级的用户可以看到高密级的信息，因此，信息内容可以无限扩散，从而使信息的保密性无法保障；但低密级的用户永远无法修改高密级的信息，从而保障信息的完整性。

2）保障信息机密性策略

与保障完整性策略相反，为了保障信息的保密性，低级别的主体不可以读高级别的信息（保密），但低级别的主体可以写高级别的客体（完整性可能破坏），因此采用的是下读/上写策略。即属于某一个安全级的主体可以写本级和本级以上的客体，但只能读本级和本级以下的客体。比如机密级主体可以写绝密级、机密级的客体，可以读机密级、秘密级、无密级的客体。这样，低密级的用户可以写高密级的信息，因此，信息完整性得不到保障：但低密级的用户永远无法看到高密级的信息，从而保障信息的保密性。

综上所述，自主访问控制技术较弱，而强制访问控制技术又太强，会给用户带来许多

不便。因此，在实际应用中，往往将自主访问控制技术与强制访问控制技术结合在一起使用。自主访问控制作为基础的、常用的控制手段；强制访问控制作为增强的、更加严格的控制手段。某些客体可以通过自主访问控制保护，重要课题必须通过强制访问控制保护。

下面介绍一个实例，UNIX 文件系统强制访问控制机制的 Multics 方案。

在 Multics 方案中，文件系统和 UNIX 文件系统一样，是一个树形结构，所有的用户和文件(包括目录文件)都有一个相应的安全级。用户对文件的访问需要遵守下述安全策略。

- 仅当用户的安全级别不低于文件的安全级别时，用户才可以读文件(下读策略)。
- 仅当用户的安全级别不高于文件的安全级别时，用户才可以写文件(上写策略)。

这就是前面详细介绍过的保密性策略。

6. 基于角色的访问控制

在传统的访问控制中，主体始终是和特定实体捆绑对应的。例如，用户以固定的用户名注册，系统给其分配一定的权限，该用户将始终以该用户名访问系统，直至销户。其间，用户的权限可以变更，但变更必须在系统管理员的授权下才能进行。然而在现实社会中，这种访问控制方式表现出很多弱点，不能满足实际需求。主要问题如下：

- 同一用户在不同的场合需要以不同的权限访问系统，按传统的做法，变更权限必须经系统管理员授权修改，因此很不方便。
- 当用户量大量增加时，按每个用户一个注册账号的方式将使得系统管理变得复杂、工作量急剧增加，也容易出错。
- 传统访问控制模式不容易实现层次化管理。即按每用户一个注册账号的方式很难实现系统的层次化分权管理，尤其是当同一用户在不同场合处的不同的权限层次时，系统管理很难实现。除非同一用户以多个用户名注册。

基于角色的访问控制模式 RBAC(Role Based Access Control)，就是为克服以上问题而提出来的。在基于角色的访问控制模式中，用户不是自始至终以同样的注册身份和权限访问系统，而是以一定的角色访问，不同的角色被赋予不同的访问权限，系统的访问控制机制只看到角色，而看不到用户。用户在访问系统前，经过角色认证而充当相应的角色。用户获得特定角色后，系统依然可以按照自主访问控制或强制访问控制机制控制角色的访问能力。

1) 角色的概念

一组特定应用的操作(或过程)称为角色(role)。在这里，角色指从事相关工作内容的一类人员，或是一组完成相同处理的相关进程。是主体从它们履行的角色上获得访问权限。

在基于角色的访问控制中，角色定义为与一个特定活动相关联的一组动作和责任。系统中的主体担任角色，完成角色规定的责任，具有角色拥有的权限。一个主体可以同时担任多个角色，它的权限就是多个角色权限的总和。基于角色的访问控制就是通过各种角色的不同搭配授权来尽可能实现主体的最小权限(最小授权指主体在能够完成所有

必需的访问工作基础上的最小权限）。

例如，在一个银行系统中，可以定义出纳员、分行管理者、系统管理员、顾客和审计员等角色。其中，担任系统管理员的用户具有维护系统文件的责任和权限，无论这个用户具体是谁。系统管理员可能是由某个出纳员兼任，他就具有两种角色。但是出于责任分离的考虑，需要对一些权利集中的角色组合进行限制，比如规定分行管理者和审计员不能由同一个用户担任。

基于角色的访问控制可以看作是基于组的自主访问控制的一种变体，一个角色对应一个组。

2）基于角色的访问控制

基于角色的访问控制就是通过定义角色的权限，为系统中的主体分配角色来实现访问控制的，其一般模型如图 4-14 所示。用户先经认证后获得一定角色，该角色被分派了一定的权限，用户以特定角色访问系统资源，访问控制机制检查角色的权限，并决定是否允许访问。

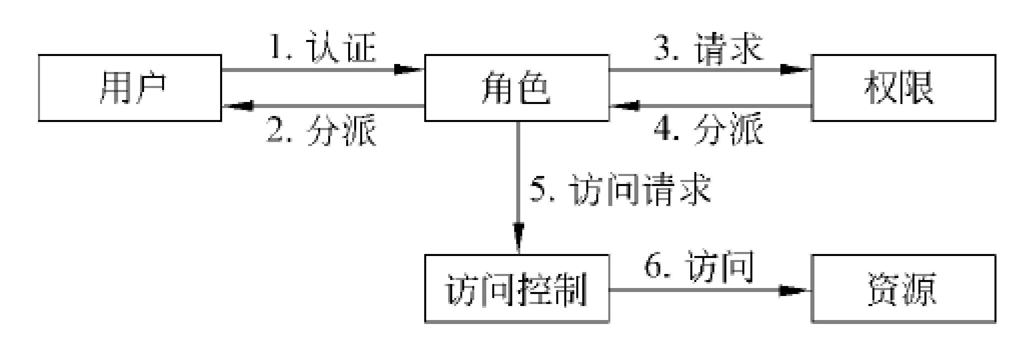


图 4-14 RBAC 模型

下面通过一个具体实例来说明基于角色的访问控制策略。例如，前面已经定义了角色的银行系统，可设计如下的访问策略。

- 允许出纳员修改顾客的账号记录（包括存款、取款和转账等），并允许出纳员询问所有账号的注册项。
- 允许分行管理者修改顾客的账号记录（包括存款、取款，但不包括规定的资金数目的范围），并允许分行管理者查询所有账号的注册项，还可以创建和取消账号。
- 允许一个顾客询问自己的注册项，但不能询问其他任何的注册项。
- 允许系统管理员询问系统注册项和开关系统，但不允许读或修改顾客的账号信息。
- 允许审计员阅读系统中所有的信息，但不允许修改任何信息。

这种策略陈述具有很明显的优势，包括如下：

- 表示方法和现实世界一致，使得非技术人员也容易理解。
- 容易映射到访问矩阵和基于组的自主访问控制，便于实现。

4.2.2 安全审计技术

1. 安全审计的目标

审计技术出现在计算机技术之前，是产生、记录并检查按时间顺序排列的系统事件记录的过程。安全审计是计算机和网络安全的重要组成部分。安全审计提供的功能服

务于直接和间接两方面的安全目标，直接的安全目标包括跟踪和监测系统中的异常事件，间接的安全目标是监视系统中其他安全机制的运行情况和可信度。

所有审计的前提是有一个支配审计过程的规则集。规则的确切形式和内容随审计过程具体内容的改变而改变。在商业与管理审计中，规则集包括对确保商业目标的实现有重要意义的管理控制、过程和惯例。这些商业目标包括资源的合理使用、利率最大化、费用最小化、符合相应的法律法规和适当的风险控制。在计算机安全审计的特殊情况下，规则集通常以安全策略的形式明确表述。并且，为了能完成合理的审计数据分析，策略表中还需要增加一些不容易明确表述的规则。

计算机安全审计是通过一定的策略，利用记录和分析历史操作事件发现系统的漏洞并改进系统的性能和安全。计算机安全审计需要达到的目的包括，对潜在的攻击者起到震慑和警告的作用；对于已经发生的系统破坏行为提供有效的追究责任的证据；为系统管理员提供有价值的系统使用日志，帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞。

James R Anderson 对计算机安全审计机制的目标作了如下阐述。

- 应为安全人员提供足够多的信息，使他们能够定位问题所在。但另一方面，提供的信息应不足以使他们自己也能够进行攻击。
- 应优化审计追踪的内容，以检测发现的问题，而且必须能从不同的系统资源收集信息。
- 应能够对一个给定的资源进行审计分析，分辨看似正常的活动，以发现内部计算机系统的不正当使用。
- 设计审计机制时，应将系统攻击者的策略也考虑在内。

概括而言，审计系统的目标至少包括如下：

- 确定和保持系统活动中每个人的责任。
- 确认重建事件的发生；评估损失。
- 监测系统问题区；提供有效的灾难恢复依据。
- 提供阻止不正当使用系统行为的依据。
- 提供案件侦破证据。

2. 安全审计系统的组成

审计是通过对所关心的事件进行记录和分析来实现的，因此审计过程包括审计发生器、日志记录器、日志分析器和报告机制几部分，如图 4-15 所示。

审计发生器的作用是在信息系统中，当各种事件发生时将这些事件的关键要素进行抽取并形成可记录的素材。日志记录器将审计发生器抽取的事件素材记录到指定的位置上，从而形成日志文件。日志分析器根据审计策略和规则对已形成的日志文件进行分析，得出某种事件发生的事实和规律，并形成日志审计分析报告。

3. 日志的内容

在理想情况下，日志应该记录每一个可能的事件，以便分析发生的所有事件，并恢复在任何时刻进行的历史情况。然而，这样做显然是不现实的，因为要记录每一个数据包、

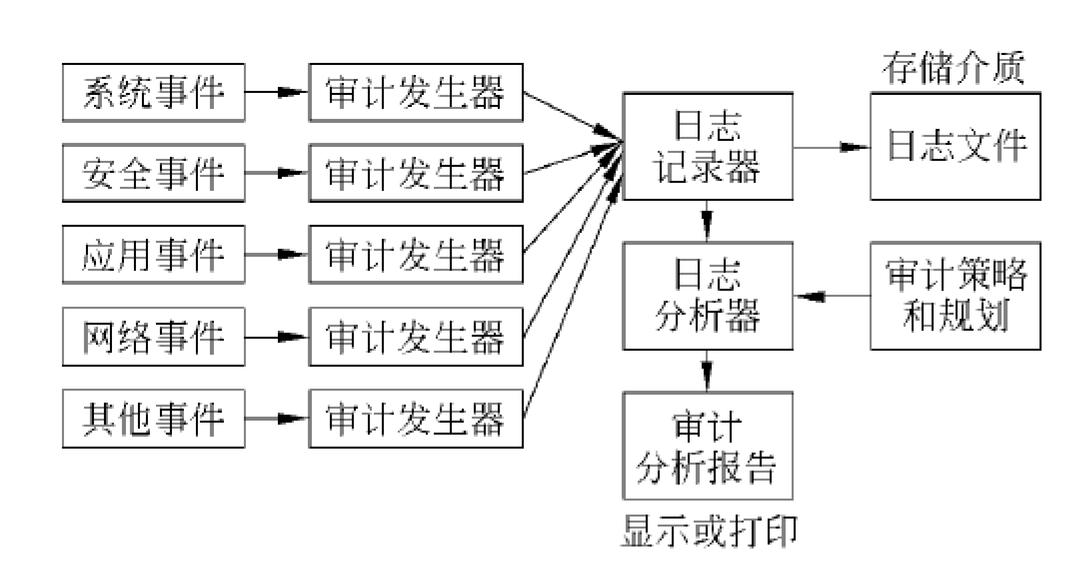


图 4-15 审计系统基本结构

每一条命令和每一次存取操作，需要的存储量将远远大于业务系统，并且将严重影响系统的性能。因此，日志的内容应该是有选择的。一般情况下，日志记录的内容应该满足以下原则。

- 日志应该记录任何必要的事件，以检测已知的攻击模式。
- 日志应该记录任何必要的事件，以检测异常的攻击模式。
- 日志应该记录关于记录系统连续可靠工作的信息。

在这些原则的指导下，日志系统可根据安全策略的要求强度选择记录下列事件。

- 审计功能的启动和关闭。
- 使用身份鉴别机制。
- 将客体引入主体的地址空间。
- 删除客体。
- 管理员、安全员、审计员和一般操作人员的操作。
- 其他专门定义的可审计事件。

通常，对于一个事件，日志应包括事件发生的日期和时间、引发事件的用户、事件的源和目的的位置、事件类型、事件成败等。

4. 安全审计的记录机制

不同的系统可采用不同的机制记录日志。日志的记录可以由操作系统完成，也可以由应用系统或其他专用记录系统完成。但是，大部分情况都可用系统调用 Syslog 来记录日志，也可以用 SNMP(简单网络管理协议)记录。

Syslog 由 Syslog 守护程序、Syslog 规则集及 Syslog 系统调用 3 部分组成，如图 4-16 所示。

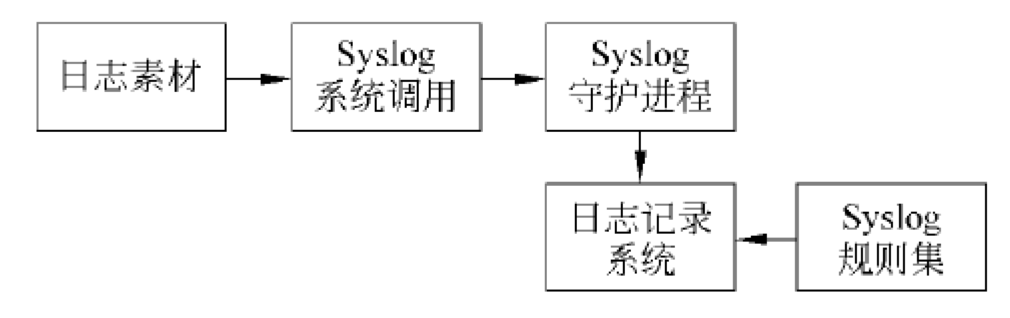


图 4-16 Syslog 记录机制

记录日志时,系统调用 Syslog 将日志素材发送给 Syslog 守护程序,Syslog 守护程序监听 Syslog 调用或 Syslog 端口(UDP514)的消息,然后根据 Syslog 规则集对收到的日志素材进行处理。如果日志是记录在其他计算机上,则 Syslog 守护进程将转发到相应的日志服务器上。Syslog 规则集是用来配置 Syslog 守护程序如何处理日志的规则。通常的规则可以是以下情况:

- 将日志放进文件中。
- 通过 UDP 将日志记录到另一台计算机上。
- 将日志写入系统控制台。
- 将日志转发给所有注册的用户。

在记录日志时,为了便于管理,通常将一定时段的日志存为一个文件。这样,就需要在 0:00 时刻切换日志文件,如图 4-17 所示。图中假设日志文件在 2006 年 5 月 15 日零点切换,此前的文件名为 logfile.20060515,此后文件名为 logfile.20060516,那么 0:00 日志监护程序会生成新文件,关闭旧文件,同时将新日志写入新文件中。

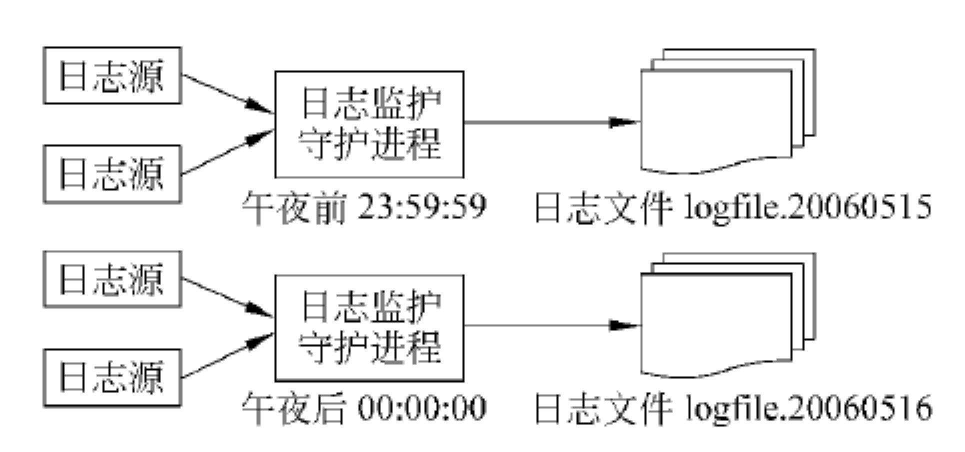


图 4-17 日志文件切换

在日志文件切换时,一种适合切换的算法是每次写文件之前打开文件,写完后关闭,程序如下:

```
While(okToRun)
  {
    Message= getlogmessage();
    FILE= openForAppending(logfile);
    Append(FILE,message);
    Close(FILE);
  }
```

值得注意的是,由于文件的打开和关闭时间较写的时间慢得多,因此可能会导致有些事件丢失。为此,可以将一个文件永久打开,供日志读写。程序如下:

```
FILE= openForAppending(logfile);
While(okToRun)
{
  Message= getlogmessage();
  Append(FILE,message);
}
Close(FILE);
```

但这样又会影响日志文件的切换。因此比较好的做法是将 Syslog 监护程序打开的文件作为原始日志文件,另外增加一个日志整理进程,专门负责日志的整理和归档。

5. 安全审计分析

通过对日志进行分析,发现所需事件信息和规律是安全审计的根本目的。因此,审计分析十分重要。日志分析就是在日志中寻找模式,主要内容如下:

1) 潜在侵害分析

日志分析应能用一些规则去监控审计事件,并根据规则发现潜在的入侵。这种规则可以是由已定义的,可审计事件的子集所指示的潜在安全攻击的积累或组合,或者其他规则。

2) 基于异常检测的轮廓

日志分析应确定用户正常行为的轮廓,当日志中的事件违反正常访问行为的轮廓,或超出正常轮廓一定的门限时,能指出将要发生的威胁。

3) 简单攻击探视

日志分析应对重大威胁事件的特征有明确的描述,当这些攻击现象出现时,能及时指出。

4) 复杂攻击探测

要求高的日志分析系统还应能检测到多步入侵序列,当攻击序列出现时,能预测其发生的步骤。

6. 审计事件查阅

由于审计系统是追踪、恢复的直接依据,甚至是司法依据,因此其自身的安全性十分重要。审计系统的安全主要是查阅和存储的安全。

审计事件的查阅应该受到严格的限制,不能篡改日志。通常通过以下不同的层次保证查阅的安全。

1) 审计查阅

审计系统以可理解的方式为授权用户提供查阅日志和分析结果的功能。

2) 有限审计查阅

审计系统只能提供对内容的读权限,因此应拒绝具有读以外权限的用户访问审计系统。

3) 可选审计查阅

在有限审计查阅的基础上限制查阅的范围。

7. 审计事件存储

审计事件的存储也有安全要求,具体有如下几种。

1) 受保护的审计踪迹存储

即要求存储系统对日志事件具有保护功能,防止未授权的修改和删除,并具有检测修改/删除的能力。

2）审计数据的可用性保证

在审计存储系统遭受意外时，能防止或检测审计记录的修改，在存储介质存满或存储失败时，能确保记录不被破坏。

3）防止审计数据丢失

在审计踪迹制超过预定的门限时，应采取相应的措施防止数据丢失。这种措施可以是忽略可审计事件、只允许记录有特殊权限的事件、覆盖以前记录、停止工作。

4.3 应用实例：RSA算法的应用

4.3.1 信息加密技术

对于公开密钥加密体制的 RSA 算法，可以用下述步骤进行算法的通俗描述。

第 1 步，给出两个任意的大素数 p,q。

第 2 步，计算：$n=p\times q$ ，$\varphi(n)=(p-1)\times(q-1)$。

第 3 步，取一个素数 e，满足 $1<e<\varphi(n)$，并且与 $\varphi(n)$互质。

第 4 步，计算 d 值：$d=(\varphi(n)\times s+1)/e$，取 $s=1,2,3\cdots,d$ 必须是整数且小于$\varphi(n)$。

第 5 步，如果 $e*d \bmod \varphi(n)=1$ 转第 6 步，否则转第 3 步，另取一个 e 值，重新计算 d 值。

第 6 步，输出 e,d。(e,n)为公开密钥，(d,n)为私有密钥。

例 4-7 RSA 算法加/解密的应用。设要将明文 $P=2$ 用发送方的私有密钥进行加密后传送给对方，对方在收到密文 C 后，再用发送方的公开密钥进行解密。设发送方用以计算密钥的两个素数是 $p=3$，$q=7$。

第 1 步，$n= p\times q=3\times 7=21$，$\varphi(n)=(p-1)\times(q-1)=2\times 6=12$

第 2 步，取 $e=5$ （这里的 e 满足 $1<e<\varphi(n)$，并且与 $\varphi(n)$互质）

第 3 步，计算 d 值：$d=(12\times s+1)/5$

当 $s=2$ 时，$d=(12\times 2+1)/5=25/5=5$

第 4 步，验证：$e\times d \bmod \varphi(n)=25 \bmod 12=1$。

发送方的加密过程：$C=P^e \bmod n \rightarrow C=2^5 \bmod 21 \rightarrow C=32 \bmod 21 =11$

接收方的解密过程：$P=C^d \bmod n \rightarrow P=11^5 \bmod 21 \rightarrow P=161\,051 \bmod 21=2$

4.3.2 数字签名技术

1. 数字签名技术

日常生活中的信件或文件是根据亲笔签名和印鉴来识别和证明其身份真实性的。但在计算机网络中，传输的文件又是如何进行身份识别和认定的呢？这就是本节所要介绍的数字签名。数字签名技术在身份认定中，特别是电子商务中有着广泛的应用前景。

数字签名必须保证做到以下 3 点。

- 接收者能够核实发送者对报文的签名。

- 发送者事后不能抵赖对报文的签名。
- 接收者不能伪造对报文的签名。

当前，有多种数字签名技术，最常用的有“RSA 加密算法签名技术”、“DSS 数字签名标准技术”、“ElGamal 数字签名技术”。在这里介绍的是“RSA 数字签名技术”。

使用公开密钥加密算法(RSA)进行数字签名的步骤如下：

发送者用其公开密钥对中的解密密钥(秘密密钥)SKA 对报文 P 进行解密运算(事实上是加密运算)，并将其运算结果 $C=D_{SKA}(P)$(数字签名)传送给接收者 B。接收者 B 收到 A 发来的数字签名 $C=D_{SKA}(P)$后，使用 A 公开的加密密钥 PKA 对其进行解密运算，即：

$$P= D_{PKA}(C)= D_{PKA}(D_{SKA}(P))$$

因为除 A 以外，没有人知道 A 的解密密钥 SKA，所以除了 A 以外，没有人能生产密文 $D_{SKA}(P)$。这样，接收方 B 就能据此来鉴别发送者 A 的身份，即相信报文 P 是 A 的数字签名后发送的。

数字签名技术如图 4-18 所示。

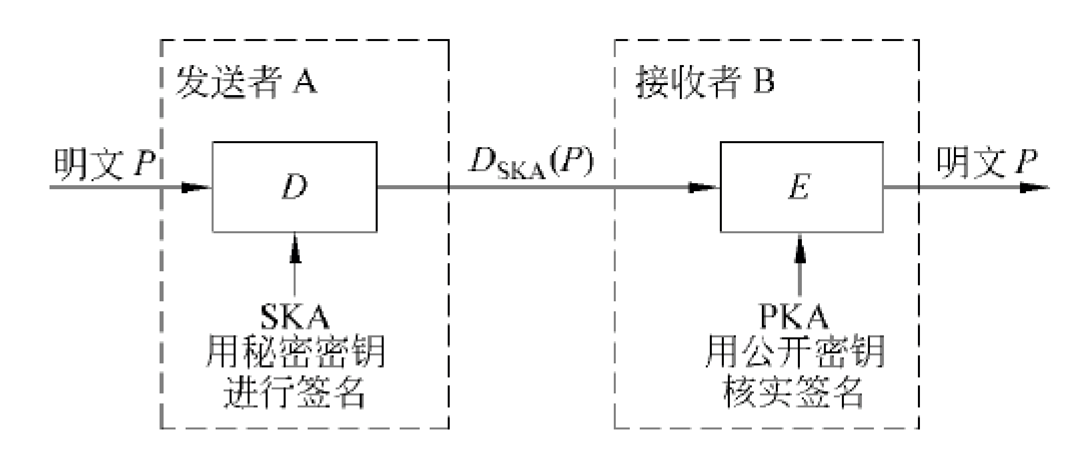


图 4-18 RSA 算法数字签名技术

2. 抗赖技术

为了进行抗赖服务，第三方权威机构必须对所有用户的公开密钥进行登记存档，以便作为抗赖服务的依据，第三方权威机构就像我们日常生活中的法院一样，是以事实为依据进行鉴别的。

经过上述签名后，若 A 要抵赖曾经给 B 发送过的报文，B 可将明文 P 及数字签名 $D_{SKA}(P)$出示给第三方权威机构。第三方很容易用 PKA 去证实 P 确实是 A 发送给 B 的。反之，若 B 将 P 伪造成 P'，则 B 不能在第三方权威机构面前提供与 $D_{SKA}(P)$ 相同的 $D_{SKA}(P')$。这样就证明了 B 伪造了报文。由此可见，实现数字签名也同时实现了对报文来源的鉴别。

上述过程仅对报文进行了签名，但对报文 P 本身却未能保密。因为凡是能截获到密文 $D_{SKA}(P)$并知道发送者身份的任何人，通过上网查阅用户名册，即可获得发送者的公开密钥 PKA，便可轻松地对 $D_{SKA}(P)$进行解密，从而能理解消息的内容。

解决这一问题的关键在于，要对报文进行二次加密。具体加密步骤是，首先发送方用自身的秘密密钥 SKA 对报文进行数字签名，产生数字签名密文 $D_{SKA}(P)$，然后再用报文接收者 B 的公开密钥 PKB 对 $D_{SKA}(P)$进行二次加密，形成密文 $E_{PKB}(D_{SKA}(P))$，之后

再发送给 B。B 收到密文 $E_{PKB}(D_{SKA}(P))$后，先用自身的秘密密钥 SKB 对其进行解密，再用 A 的公开密钥 PKA 核实数字签名，如图 4-19 所示。

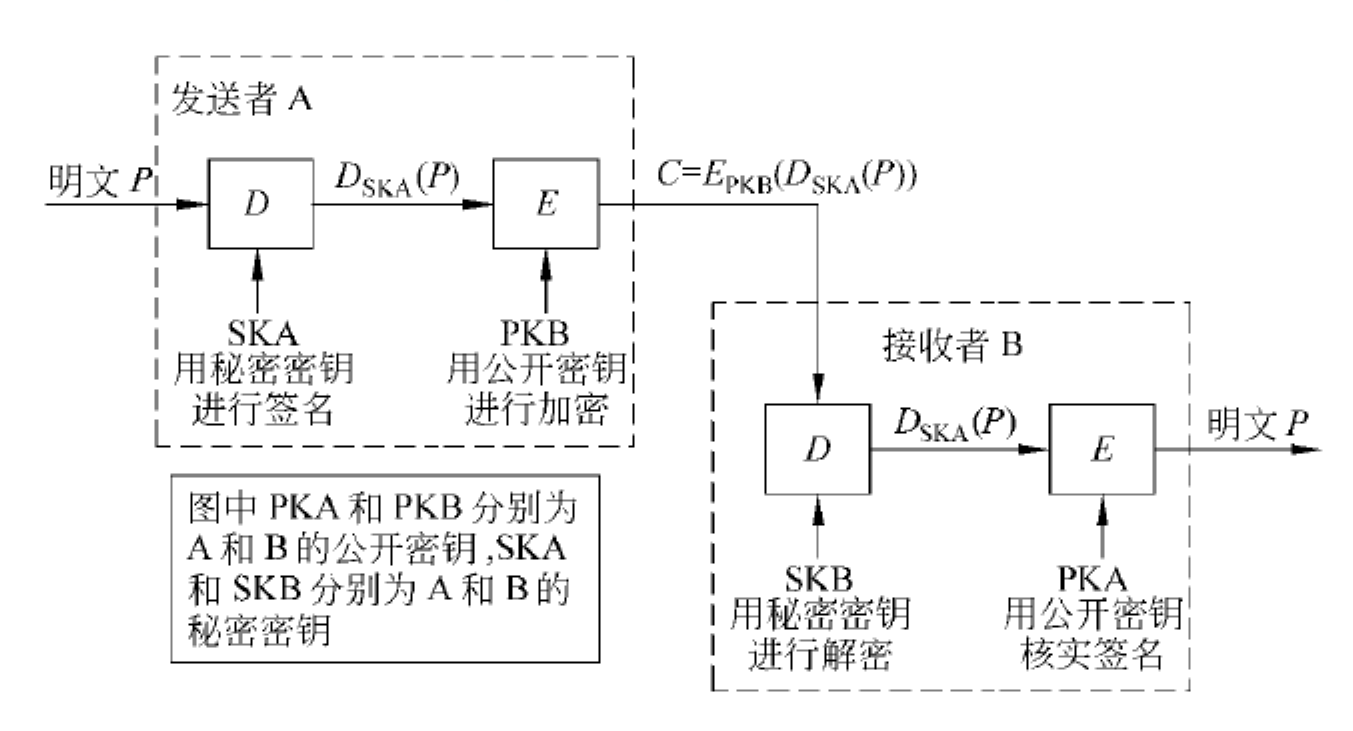


图 4-19　RSA 数字签名技术

由于第三方无法获得 B 的秘密密钥 SKB，即使第三方窃取了密文 $E_{PKB}(D_{SKA}(P))$，并知道 A、B 双方的公开密钥 PKA 和 PKB，仍然是无法对 $E_{PKB}(D_{SKA}(P))$进行解密。这就保证了数字签名的保密性和可行性。

例 4-8　数字签名实例。

设用户 A(用户身份代号为 2)：取 $p=3, q=11, n=33, \varphi(n)=20, e=3, d=7$

$$PKA=(3,33),\quad SKA=(7,33)$$

用户 B(用户身份代号为 3)：取 $p=5, q=11, n=55, \varphi(n)=40, e=7, d=23$

$$PKB=(7,55),\quad SKB=(23,55)$$

A 方：数字签名并加密(用户 A 的代号为 2，数字 2 即是 A 的身份)。

$$C = E_{PKB}(D_{SKA}(P)) = E_{PKB}(2^7 \bmod 33) = E_{PKB}(29)$$
$$=29^7 \bmod 55=39$$

B 方：先解密再进行签名核实。

$$P = D_{PKA}(D_{SKB}(C)) = D_{PKA}(39^{23} \bmod 55) = D_{PKA}(29)$$
$$=29^3 \bmod 33 = 2$$

3. 数字证书和公钥基础设施(PKI)

数字证书就是网络通信中标志通信各方身份信息的一系列数据，其中包括本人的公开密钥。数字证书是由一个权威机构发行的，它类似于现实生活中的身份证。一个数字证书由 3 部分组成：

- 公开密钥。
- 证书信息(用户的身份)。
- 一个或多个数字签名。

对证书进行发行、存储、查询的结构化系统叫公钥基础设施 PKI(Public Key Infrastructures)，PKI 通过一个权威的认证中心 CA(Certification Authority)去发行数字证

书,CA 认证中心是 PKI 的核心。

4.3.3 数字信封技术

由于公开密钥加密体制的加密和解密速度慢,在实际应用中,除了数字签名以外,很少用公开密钥算法来加密数据。通常是用对称密钥来加密数据,而用公开密钥算法来加密对称加密算法的密钥,这就是本小节要介绍的“数字信封技术”。

数字信封技术是用来保证数据在传输过程中的安全。传统的对称加密方法的算法运算效率高,但是密钥不适合通过公共网络传送,而非对称加密算法的密钥传送简单,但加密算法的运算效率低。数字信封技术则是将传统的对称加密算法与现代的非对称加密算法(公开密钥加密算法)结合起来,充分利用了对称加密算法的高效性和大量对称加密算法的灵活性,以保证信息在传输过程中的安全性。图 4-20 给出了数字信封技术的工作流程。

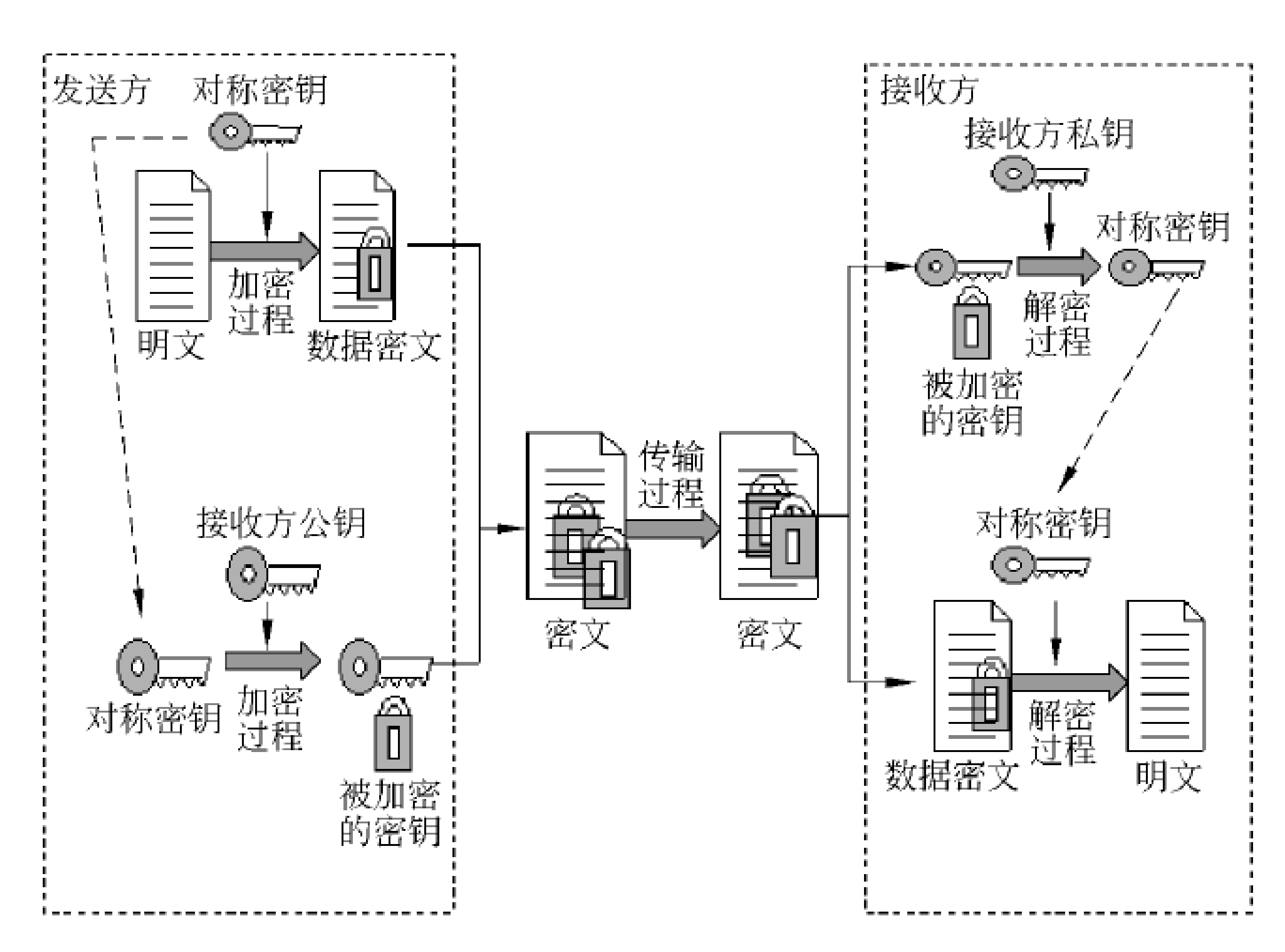


图 4-20　数字信封技术的工作流程图

从图 4-20 中可看出,在数字信封技术中需要两个不同的加密解密过程,数据本身的加密和解密、密钥的加密和解密。首先,使用的是对称加密算法对需发送的数据进行加密,然后再利用非对称加密算法对对称加密的密钥进行加密和解密。其加密解密过程如下:

第 1 步,在需要发送信息时,发送方生成一个对称密钥。

第 2 步,发送方使用一个对称加密的密钥和算法对需发送的数据进行加密,形成加密的数据密文。

第 3 步,发送方使用接收方提供的公开密钥,对发送方的对称密钥进行加密。

第 4 步,发送方通过网络将加密后的密文和加密后的对称密钥传输给接收方。

第 5 步,接收方用自身的私有密钥对接收到的对称密钥进行解密,得到对称密钥。

第 6 步，接收方使用解密后的对称密钥对数据密文进行解密，得到明文数据。

数字信封技术使用的是两层加密体制，在内层利用了对称加密技术，每次传送的信息都可以重新生成新的密钥，保证信息的安全性，在外层，利用非对称加密技术加密对称密钥，保证了密钥传送的安全性。

4.3.4 身份认证技术

身份认证是信息安全理论的重要组成部分。以密码理论为基础的身份认证是访问控制和审计的前提，因此对网络环境下的信息安全尤其重要。本节重点讲述身份认证的作用、原理和实现技术。

认证协议按照认证的方向可以分为双向认证协议和单向认证协议，按照使用的密码技术可以分为基于对称密码的认证协议和基于公钥密码的认证协议。

1. 双向认证协议

双向认证就是使通信双方确认对方的身份，适用于通信双方同时在线的情况。

1）基于对称密码的双向认证协议

Needham/Schroeder 是一个基于对称加密算法的协议，它要求有可信任的第三方 KDC（密钥分配中心）参与，采用 Challenge/Response（提问/应答）的方式，使得 A、B 互相认证对方的身份。协议过程是：

第 1 步，A→KDC：$ID_A \parallel ID_B \parallel N_1$。

第 2 步，KDC→A：$E_{ka}[ks \parallel ID_B \parallel N_1 \parallel E_{kb}[Ks \parallel ID_A]]$。

第 3 步，A→B：$E_{kb}[ks \parallel ID_A]$。

第 4 步，B→A：$E_{ks}[N_2]$。

第 5 步，A→B：$E_{ks}[f(N_2)]$。

其中，KDC 是密钥分发中心；ID_A 表示 A 身份的唯一标识、ID_B 表示 B 身份的唯一标识；密钥 Ka 和 Kb 分别是 A 与 KDC、B 与 KDC 之间共享的密钥；N_1 和 N_2 是两个 nonce（现时值）：$f(N)$是对 N 进行一个运算，比如 $f(N)=N+1$。本协议的目的是认证 A 和 B 的身份后，安全地分发一个会话密钥 Ks 给 A 和 B。

说明：

第 1 步，A 向 KDC 申请要和 B 通信的申请要求。

第 2 步，A 安全地得到了一个新的会话密钥 ks。

第 3 步，A 用 B 方的公开密钥加密会话密钥 ks 和 A 的身份标识 ID_A（数字签名），这条消息只能由 B 解密并理解，B 也获得会话密钥。

第 4 步，B 相信了 A 的身份后，用对称密钥 Ks 加密一个现时值 N_2 发送给 A，即 B 告诉 A 已知道正确的 Ks，从而证明了 B 的身份。

第 5 步，A 对 B 发来的 $E_{ks}[N_2]$进行解密，证明 B 的身份后，再给 B 发送一条确认信息。之后，双方就可以通信了。

第 4、5 两步的目的是为了防止某种类型的重放攻击，特别是如果攻击方能够在第 3 步捕获该消息并进行重放，这将在某种程度上干扰破坏 B 方的运行操作。

由于除了KDC之外只有A知道Ka,也只有B知道Kb,所以双方都可以向对方证明自己的身份。

但是,这个协议仍然有漏洞。假定攻击方C已经掌握A和B之间通信的一个老的会话密钥,C可以在第3步冒充A,利用老的会话密钥欺骗B。除非B记住所有以前使用的与A通信的会话密钥,否则B无法判断这是一个重放攻击。然后,如果C可以中途阻止第4步的握手信息则可以冒充A在第5步响应。从这一点起C就可以向B发送伪造的消息,而B认为是在与A进行正常的通信。

为解决这一问题,Deming结合了时间戳的方法,对会话协议的算法进行了改进。

第1步,A→KDC:$ID_A \| ID_B$。

第2步,KDC→A:$E_{ka}[ks \| ID_B \| T \| E_{kb}[Ks \| ID_A \| N_1]]$。

第3步,A→B:$E_{kb}[ks \| ID_A \| T]$。

第4步,B→A:$E_{ks}[N_1]$。

第5步,A→B:$E_{ks}[f(N_1)]$。

$$|\text{Clock} - T| < \Delta t_1 + \Delta t_2$$

其中,T是时间戳;Δt_1是KDC时钟与本地时钟(发送方A所在地)之间差异的估计值;Δt_2是预期的网络延迟时间。

如果发送者的时钟比接收者的时钟要快,攻击者就可以从发送者处窃听消息,并等待时间戳对接收者来说成为当前时刻时重放给接收者,这种重放将会得到意想不到的后果。这一类型的重放攻击又称“抑制重放攻击”。

2)基于公钥密码的双向认证协议

使用公钥密码算法,可以克服基于对称密码的认证协议中的一些问题。但同样需要有可信的第三方参与,现以WOO92b协议为例加以说明如下:

第1步,A→KDC:$ID_A \| ID_B$。

第2步,KDC→A:$E_{KRauth}[ID_B \| KU_{kb}]$。

第3步,A→B:$E_{KUb}[N_a \| ID_A]$。

第4步,B→KDC:$ID_B \| ID_A \| E_{KUauth}[N_a]$。

第5步,KDC→B:$E_{KRauth}[ID_A \| KU_a] \| E_{KUb}[E_{KRauth}[N_a \| Ks \| ID_A \| ID_B]]$。

第6步,B→A:$E_{KUa}[E_{KRauth}[N_a \| Ks \| ID_A \| ID_B \| N_b]]$。

第7步,A→B:$E_{ks}[N_b]$。

其中,KUa是A的公钥,KRa是A的私钥,KUauth是KDC的公钥,KRauth是KDC的私钥。

说明:

第1步,A向KDC提出要与B通信的要求。

第2步,A从KDC得到B的公钥。

第3步,A向B提出通信要求,信息中包含一个现时信息N_a。

第4步,B向KDC询问A的公钥。

第5步,B得到A的公钥和一段KDC签名的消息。

第6步,B将这段消息和现时N_b发给A,A在KDC签名的消息中找到N_a,确认这

不是一个重放。

第 7 步，A 使用刚得到的会话密钥回答 B。

在协议中，A 和 B 都向 KDC 索取对方的公钥，如果对方能正确解密用其公钥加密的消息，就能够证明对方的身份。

2. 单向认证协议

大多数单向认证的应用是不需要双方同时在线的，一方在向另一方证明自己的身份的同时，即可发送数据；对方收到身份认证消息及其数据后，首先验证发送方的身份，如果身份有效，则可以接收数据，否则拒绝接收。

1）基于双方在线的单向认证协议

单向认证协议中只有一方向另一方证明自己的身份，因此过程一般都相对简单。下面是一个不需要第三方的基于对称密码的单向认证协议，要求 A 和 B 事先拥有共享密钥。

第 1 步，A→B：$ID_A \parallel N_1$。

第 2 步，B→A：$E_{Kab}[Ks \parallel ID_B \parallel f(N_1) \parallel N_2]$。

第 3 步，A→B：$E_{ks}[f(N_2)]$。

说明：

第 1 步，A 将自己的身份 ID_A 和一个一次性随机数 N_1(nonce)发给 B，希望和 B 建立通信连接。

第 2 步，B 生成一个会话密钥 Ks，连同对 Anonce 应答和一个新的 nonce，一起用双方的共享密钥加密后发给 A。

第 3 步，A 对 B 发过来的现时值进行解密，并验证 B 的身份，当 B 的身份得到确认后，A 计算出第二个 nonce 的应答，用 Ks 加密后发给 B，B 收到后如果能正确解密出应答，则说明 A 的身份是可信的，因为只有 A、B 双方拥有共享密钥 Kab。之后，A 即可向 B 发送数据。

2）基于 KDC 的单向认证协议

上述方案的缺点是双方必须同时在线，不适合于单方在线的情况。基于第三方（密钥分配中心 KDC）的应答方案可以有效地解决这一问题，第三方一般是长期在线的、双方信赖的权威机构。

第 1 步，A→KDC：$ID_A \parallel ID_B \parallel N_1$。

第 2 步，KDC→A：$E_{Ka}[Ks \parallel ID_B \parallel N_1 \parallel E_{Kb}[Ks \parallel ID_A]]$。

第 3 步，A→B：$E_{Kb}[Ks \parallel ID_A] \parallel E_{ks}[(M)]$。

说明：

第 1 步，A 向 KDC 要求和 B 通信，同时发给 KDC 一个 nonce。

第 2 步，KDC 发给 A 一个用 A 的密钥加密的消息，包括一个会话密钥 Ks、A 发送的 nonce、一段用 B 的密钥加密的消息；同时 A 解密得到 Ks。

第 3 步，A 将用 B 的密钥加密的那段消息和用 Ks 加密的数据一起发送给 B；B 收到后首先解密得到 A 的身份标识 Ks，然后就可以解密 A 发来的数据了。

这种方案的好处在于不要求 B 同时在线，其缺点是不能防止重放攻击，因在第 3 步中，B 收到消息后不能确认这一消息是 A 发送的消息还是重放的消息。

3）基于公钥的单向身份认证协议

基于公钥的单向身份认证协议非常简单，基认证过程只要一个步骤。

A→B: $E_{KUb}[Ks] \| E_{Ks}[M \| E_{KRa}[H(M)]]$。

这种方案要求 A 和 B 互相知道对方的公钥。首先，A 用 B 的公钥加密一个会话密钥，然后 A 用会话密钥加密数据和用自己私钥签名的消息摘要，A 将这些内容一起发送给 B。B 收到后，首先用自己的私钥解密出会话密钥，然后解密消息和 A 的签名，最后计算出消息摘要以验证 A 的签名，从而确定 A 的身份。

习 题 4

一、概念题

1. 信息安全的目标是什么？
2. 保护信息机密性的含义是什么？
3. 抗否认服务的含义是什么？如何实现抗否认服务？
4. 访问控制的目的是什么？
5. 单表代换密码、多表代换密码、多字母密码代换的含义是什么？它们之间有什么区别？
6. 分组密码加密算法和流密码加密算法有何区别？
7. 消息摘要算法的基本思想是什么？其目的是什么？
8. 公开密钥加密体制和对称密钥加密体制各自的加密/解密思想是什么？
9. 公开密钥体制具有什么样的特点？
10. 访问控制策略是什么？
11. 访问控制一般包括哪些类型？
12. 安全审计过程由哪几个部分组成？
13. 数字签名应具有哪些特点？
14. RSA 算法的用途是什么？

二、计算及程序设计题

1. 设 a～z 的编号为 01～26，空格为 27，采用 Kaesar 密码方案，算法 $C=k_1M+k_2$，取 $k_1=3$，$k_2=5$，$M=$Peking University，计算密文 C。

2. 设 a～z 的编号为 1～26，空格为 27，采用 Vigenere 密码方案，密钥长度与消息相同，给出密文：

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

分别找出对应下列两组明文的密钥：

a）MR MUSTARD WITH THE CANDLESTICK IN THE HALL

b）MISS SCARLET WITH THE KNIFE IN THE LIBRARY

密钥：a）OWKLULRXCNETXQUYVBZSMKDAMDBUFCTO GEYYKLMXHG

b）OESFOLHXCF WFNTEGJDZHGRUK OIOXQOPM RUGJCXBU

3．DES 算法的应用。设密钥为“SECURITY”，明文为“NETWORK INFORMATION SECURITY”，用 DES 算法编写程序计算其密文，并列出每一轮的中间结果。

4．RSA 算法计算技巧编程。计算 17^{560} mod 561 的值。

5．RSA 算法的应用。

设 $p=3$、$q=5$、$M=2$，计算出 n、e、d，并将明文 M 用 RSA 算法加密和解密。

6．数字签名技术的应用。

设用户 A 和用户 B 的用户代号分别为 101 和 102。并设：

用户 A：$p=11$　　$q=17$

用户 B：$p=7$　　$q=17$

- 计算出 A、B 双方的公开密钥和秘密密钥。
- 用户 A 用其自身的用户代号(101)作为身份向 B 发出一条数字签名消息，要求用 B 的公开密钥进行加密。
- 对该数字签名进行解密和身份验证。
- 要求先写出数字签名和身份验证的过程，再编制程序运算。

第 5 章 chapter 5

通信安全技术

本章着重介绍在计算机网络通信过程中的拥塞控制技术、流量控制技术、差错控制技术、数据传输技术及网络死锁的防范处理技术。

5.1 拥塞控制与流量控制

网络过载，会造成网络拥塞，影响网络通信效率，严重时，会造成网络瘫痪。因此，必须对网络流量进行有效的控制。

5.1.1 网络拥塞的基本概念

当加载到某个网络上的载荷超过其处理能力时，就会出现拥塞现象。

拥塞现象应用物理层的规则便可以得到控制，这个规则即分组保持规则。就是只有当一个旧的分组被发送出去后再向网络注入新的分组。TCP 试图通过动态地控制滑动窗口的大小达到这一目的。

控制拥塞首先要做的是检测。分组丢失而造成超时有两个原因，一个是由于传输线路上的噪声干扰；另一个是拥塞的路由器丢失分组。

由于传输错误造成分组丢失的情况相对较少，因为大多数长距离的主干线都是光纤。因此，Internet 上发生的超时现象大多数都是由于拥塞造成的。Internet 上所有的 TCP 算法都假设分组传输超时是由拥塞造成的，并且以监控定时器超时作为出现问题的信号。

当数据从一个大的管道向一个较小的管道（比如一个是高速局域网而另一个是低速的广域网）发送数据时便会发生拥塞。当多个输入流到达一个路由器，而路由器的输出流小于这些输入流的总和时也会发生拥塞。

通过上述分析可知，网络产生拥塞的根本原因在于用户提供给网络的负载超过了网络的存储和处理能力，表现为无效数据包增加、报文时延增加与报文丢失、服务质量降低等。如果不能采取有效的检测和控制手段，就会导致拥塞逐渐加重，甚至造成系统崩溃，在一般情况下形成网络拥塞的三个直接原因如下：

- 路由器存储空间不足。几个输入数据流需要同一个输出端口，如果入口速率之和

大于出口速率，就会在这个端口上建立队列。如果没有足够的存储空间，数据包就会被丢弃，对突发数据流更是如此。增加存储空间在表面上似乎能解决这个矛盾，有研究表明，如果路由器有无限存储量时，拥塞只会变得更坏，这是因为，该路由器缓冲区中将会有越来越多的数据包在排队而无法传送出去。

- 带宽容量相对不足。直观地说，当数据总的输入带宽大于输出带宽时，在网络低速链路处就会形成带宽瓶颈，网络就会发生拥塞，相关证明可参考香农信息理论的有关资料。
- 处理器处理能力较弱。如果路由器的 CPU 在执行排队缓存、更新路由表等操作时，处理速度跟不上高速链路，会产生拥塞。同理，低速链路对高速处理器也会产生拥塞。

5.1.2 网络拥塞控制技术

1. 慢启动算法

综上所述，在 Internet 上存在网络的容量和接收方的容量两个潜在问题，它们需要分别进行处理。为此，每个发送方均保持两个窗口，接收方承认的窗口和拥塞窗口。每个窗口都反映出发送方可以传输的字节数。取两个窗口的最小值作为可以发送的字节数。这样，有效窗口便是发送方和接收方分别认为合适的窗口中最小的一个窗口。

当建立连接时，发送方将拥塞窗口大小初始化为该连接所有最大报文段的长度值，并随后发送一个最大长度的报文段。如果该报文段在定时器超时之前得到了确认，那么发送方在原拥塞窗口的基础上再增加一个报文段的字节值，使其为两倍最大报文段的大小，然后发送。当这些报文段中的每一个都被确认后，拥塞窗口大小就再增加一个最大报文段的长度。

当拥塞窗口是 N 个报文段的大小时，如果发送的所有 N 个报文段都被及时确认，那么将拥塞窗口大小增加 N 个报文段所对应的字节数目。

拥塞窗口保持指数规律增大，直到数据传输超时或者达到接收方设定的窗口大小。也就是说，如果发送的数据长度序列，如 1024、2048 和 4096 字节都能正常工作，但发送 8192 字节数据时出现定时器超时，那么拥塞窗口应设置为 4096 以避免出现拥塞。只要拥塞窗口保持为 4096 字节，便不会再发送超过该长度的数据量，无论接收方赋予多大的窗口空间亦是如此。这种算法是以指数规律增加的，通常称为慢启动算法。所有的 TCP 实现都必须支持这种算法。

慢启动算法工作过程如下：

慢启动为发送方的 TCP 增加了一个窗口，即拥塞窗口。当与另一个网络的主机建立 TCP 连接时，拥塞窗口被初始化为 1 个报文段（即另一端通告的报文段大小）。每收到 1 个 ACK，拥塞窗口就增加 1 个报文段（拥塞窗口以字节为单位，但是慢启动以报文段大小为单位进行增加）。发送方取拥塞窗口与接收方窗口中的最小值作为发送上限。拥塞窗口是发送方使用的流量控制，而接收方窗口则是接收方使用的流量控制。

在某些点上可能达到了因特网的容量，于是中间路由器开始丢弃分组，并通知发送

方其固有的拥塞窗口开得过大，应缩小发送窗口。

2. 拥塞避免算法

慢启动算法不能解决的问题是，数据传输达到中间路由器的极限时，分组将被丢弃。拥塞避免算法是一种处理丢失分组的最佳方法。

该算法假定由于分组受到损坏引起的丢失是极少的，因此分组丢失就表明在源主机和目的主机之间的某处网络上发生了拥塞。

常用的拥塞避免算法如下：

1）先进先出算法（First In First Out，FIFO）

传统的先进先出策略是目前 Internet 上使用最广泛的一种服务模型。它的最大优点是便于实施，但由于 FIFO 本质上是一种"去尾"（Drop-tail）的算法，所以当突发性数据到达时容易出现包丢失现象，其公平性较差，对上层的 TCP 快速恢复的效率也较低。

2）随机早期检测算法（Random Early Detection，RED）

RED 算法是按一定概率丢弃进入路由器的数据包。RED 的早期设计思路是避免丢弃属于同一连接的连续数据包，从而提高连接的吞吐量。通过分摊包丢失率，RED 可以在各连接之间获得较好的公平性，对突发业务的适应性较强。RED 也存在一些不足，例如可能会引起网络的不稳定，而且选择合适的配置参数也不是一件容易的事。近年来，研究者提出了许多 RED 的改进算法，这些算法都在一定程度上，从不同方面改善了 RED 的性能。

3）显示拥塞指示算法（Explicit Congestion Notification，ECN）

前面两种拥塞控制算法都是通过包丢失来告诉端系统，网络已经发生拥塞。而显示拥塞指示算法通过明确的拥塞提示（RFC2481）来实现拥塞控制，对一次性大批量数据传输的效果比较理想，但对时延有一定要求。

该算法在源端数据包中嵌入 ECN，由路由器根据网络情况设置 CE（Congestion Experienced）比特位。源端接收到从网络中反馈回来的这种 CE 置位数据包后，将随后发出的数据包标记为可丢弃的数据包。ECN 的优势在于不需要超时重传，也不依赖于粗粒度的 TCP 定时，所以在对时延有一定要求的应用场合性能较好。在此基础上还提出了另一种改进算法，它通过调整拥塞窗口的大小，纠正有长时间 RTT 的 TCP 连接的偏差，来改进共享瓶颈处带宽的公平性。

4）公平排队算法（Fair Queuing，FQ）

在 FQ 算法中路由器对每个输出线路都建有一个排队队列。当一条线路空闲时，路由器就来回扫描所有队列，依次将每队的第一个包发出。FQ 的带宽分配独立于数据包大小，各种服务在队列中几乎同时开始。因此在没有牺牲统计复用的情况下提供了另外的公平性，与端到端的拥塞控制机制可以较好地协同工作。它的缺点在于实现起来很复杂，需要每个数据流的排队处理、每个流的状态统计、数据包的分类以及包调度的额外开销等。

5）加权公平排队算法（Weighted Fair Queuing，WFQ）

加权公平排队算法是 FQ 的改进算法。根据不同数据流及不同带宽的要求，对每个

排队队列采用加权方法分配缓存资源，从而增加 FQ 对不同应用的适应性，该算法还有其他一些改进算法。

6）加权随机先期检测（Weighted Random Early Detection，WRED）

加权随机先期检测是将随机先期检测与优先级排队结合起来，这种结合为高优先级分组提供了优先通信服务能力。当某个接口开始出现拥塞时，它有选择丢弃优先级较低的分组，而不是随机丢弃分组。

7）定制排队

定制排队是为允许具有不同最低带宽和延迟要求的应用程序共享网络而设计的。定制排队为不同协议分配不同的队列空间，并以循环方式处理队列，当特定协议的数据流被分配了较大的队列空间，也就获得了较优先的服务，定制排队比优先级队列更为公平。定制排队可以保证每一个特定的通信类型得到固定的可用带宽，同时在链路紧张的情况下，避免了数据流企图超出预分配量限制的可能。

3. 慢启动算法＋拥塞避免算法

拥塞避免算法和慢启动算法是目的不同的、独立无关的算法。但是当拥塞发生时，为了降低分组进入网络的传输速率，可使用调用慢启动来解决拥塞。在实际中应用中，这两个算法通常在一起使用，其使用技术描述如下：

- 对一个给定的连接，初始化拥塞窗口为 1 个报文段，门限为 65 535 字节。
- TCP 输出例程的输出不能超过拥塞窗口和接收方窗口的大小。拥塞避免是发送方使用的流量控制，而接收方窗口则是接收方进行的流量控制。前者是发送方对网络拥塞的估计，而后者则与接收方在该连接上的可用缓存大小有关。
- 当拥塞发生时（超时或收到重复确认），门限被设置为当前窗口大小的一半（拥塞窗口和接收方窗口大小的最小值，但最少为 2 个报文段）。此外，如果是超时引起了拥塞，则拥塞窗口被设置为 1 个报文段（这就是慢启动）。
- 当新的数据被对方确认时，就增加拥塞窗口，但增加的方法依赖于是否正在进行慢启动或拥塞避免。如果拥塞窗口小于或等于门限，则正在进行慢启动；否则正在进行拥塞避免。

慢启动一直持续到当拥塞发生之初所处窗口大小的一半时才停止，然后才转去执行拥塞避免。

慢启动只是采用了比引起拥塞更慢些的分组传输速率，但在慢启动期间进入网络的分组数的速率仍然在增加。只有在达到门限拥塞避免算法起作用时，这种速率才会慢下来。

4. 快速重传与快速恢复算法

如果连续收到 3 个或 3 个以上的重复确认信号 ACK，就表明有一个报文段丢失了。于是还需重传丢失的数据报文段，而无须等待超时定时器溢出。这就是快速重传算法。

由于接收方只有在收到另一个相同的报文段时才产生重复的 ACK，而该报文段已经离开了网络并进入了接收方的缓存。也就是说，在收、发两端之间仍然有流动的数据，

而不执行慢启动来突然减少数据流。

快速重传与快速恢复算法步骤如下：

步骤1，当收到第3个重复的ACK时，将门限设置为当前拥塞窗口的一半，同时，重传丢失的报文段。设置拥塞窗口为门限加上3倍的报文段大小。

步骤2，每次收到另一个重复的ACK时，拥塞窗口增加1个报文段大小，并发送1个分组（如果新的拥塞窗口允许发送）。

步骤3，当下一个确认数据的ACK到达时，设置拥塞窗口为门限（在步骤1中设置的值）。这个ACK应该是在进行重传后的一个往返时间内对步骤1中重传的确认。另外，这个ACK也应该是对丢失的分组和收到的第1个重复的ACK之间的所有中间报文段的确认。

这一步骤采用的是拥塞避免算法，因为当分组丢失时该算法能将当前的速率减半。

5.1.3 流量控制技术

在数据链路层及高层协议中，一个最重要的控制技术就是流量控制技术。所谓流量控制，就是如何处理发送方的发送能力比接收方的接收能力大的问题，即当发送方在一个相对快速或负载较轻的网络上运行，而接收方在一个相对慢速或负载较重的网络上运行时。如果发送方不断地高速将数据包发出，最终会“淹没”接收方的数据包（即后传来的包会“冲掉”前面已接收但还未来得及处理的数据包），即便传输过程毫无差错，到一定的时刻，接收方将无能力处理刚收到的包，就会发生信息“丢失”的现象，因此，必须采取有效的技术与措施来防止这种丢失包的情况发生。

最常见的方法是引入流量控制来限制发送方发出的数据流量，使其发送速率不超过接收方处理的速率。这种限制流量需要某种反馈机制，使发送方了解接收方的处理速度是否能够跟上发送方发送包的速度。

流量控制协议中包括一些定义完整的规则，这些规则描写了接收方在什么时候接收下一包，在未获得接收方直接或间接允许之前，发送方禁止发出包。

5.2 差错控制技术

5.2.1 差错的基本概念

1. 差错

所谓差错就是在数据通信中，接收端接收到的数据与发送端发出的数据出现不一致的现象。差错包括如下：

- 数据传输过程中有位丢失。
- 发出的位值为0而接收到的位值为1或发出的位值为1而接收到的位值为0。即发出的位值与接收到的位值不一致。

2. 热噪声

这里所说的噪声是指不正常的干扰信号。在网络通信中要尽量避免噪声或减少噪声对信号的影响。

热噪声是影响数据在通信介质中正常传输的各种干扰因素。数据通信中的热噪声主要包括如下：

- 在数据通信中，信号在物理信道上因线路本身电气特性随机产生的信号幅度、频率、相位的畸形和衰减。
- 电气信号在线路上产生反射造成的回音效应。
- 相邻线路之间的串线干扰。
- 大气中的闪电、电源开关的跳火、自然界磁场的变化以及电源的波动等外界因素。

热噪声分为两大类，随机热噪声和冲击热噪声。

- 随机热噪声是通信信道上固有的，持续存在的热噪声。这种热噪声具有不固定性，所以称为随机热噪声。
- 冲击热噪声是由外界某种原因突发产生的热噪声。

3. 差错的产生

数据传输中所产生的差错都是由热噪声引起的。由于热噪声会造成传输中的数据信号失真，产生差错。所以在传输中要尽量减少热噪声。

4. 差错控制

差错控制就是指在数据通信过程中，发现差错、检测差错，对差错进行纠正，从而把差错尽可能限制在数据传输所允许的误差范围内所采用的技术和方法。

5. 差错控制编码

差错控制的核心是差错控制编码。差错控制编码的基本思想是通过对信息序列实施某种变换，使原来彼此独立、没有相关性的信息码元序列，经过变换产生某种相关性，接收端据此相关性来检查和纠正传输序列中的差错。不同的变换方法构成不同的差错控制编码。

用以实现差错控制的编码分为检错码和纠错码两种。检错码是能够自动发现错误但不能自动纠错的传输编码；纠错码是既能发现错误，又能自动纠正传输错误的编码。

5.2.2 差错控制方法

差错控制方法主要有自动请求重发、向前纠错和反馈校验法。

1. 自动请求重发

自动请求重发（Automatic Repeat Request System，ARRS）又称检错重发。它是利用编码的方法在数据接收端自动检测错误码，当检测出错误数据包后，通知数据发送端

重新发送错误的数据包。ARRS 的特点是只能检测出有无误码，但确定不出误码的准确位置，ARRS 技术需要系统具备双向信道。

2. 向前纠错

向前纠错(Forward Error Correct，FEC)是利用编码方法，在接收端不仅能对接收的数据进行检测，而且当检测出错误码后能自动进行纠正。FEC 的特点是接收端能够准确地确定错误码的位置，从而可自动进行纠错。应用 FEC 不需要反向信道，不存在重发延时问题，所以实时性强，但纠错设备比较复杂。

3. 反馈校验法

反馈校验法(Feedback Verify Method，FVM)是接收端将收到的信息码原封不动地发回发送端，再由发送端用反馈回来的信息码与原发信息码进行比较，如果发现错误，发送端进行重发。反馈校验的特点是其方法、原理和设备都比较简单，但需要系统提供双向信道，因为每一个信息码都至少传输两次，所以传输效率低。

4. 检错编码方法

差错检测方法很多，比如奇偶校验检测、水平垂直奇偶校验检测、定比检测、正反检测、循环冗余检测及海明检测等方法。所有这些方法分别采用了不同的差错控制编码技术。下面介绍几种常用的检错控制编码方法。

1) 垂直奇偶校验法

垂直奇偶校验是以字符为单位进行校验的方法。以 ASCII 码为编码的字符为例，一个字符由 8 位组成，其中低 7 位是信息位，最高位是校验位。

奇校验的规则是，确保发出的一组信息码中含 1 的个数为奇数；偶校验的规则是，确保发出的一组信息码中含 1 的个数为偶数。

例 5-1 如果一个字符的 7 位信息码为 1001101，采用奇校验编码，求其校验位的值。

由于这个字符的 7 位代码中有 1 的个数为偶数(4 个)，所以其校验位的值为 1。即整个 8 位发送编码为 11001101(最高位为校验位)。

当接收端接收到字符 8 位编码后，即开始检测，若检测出其含 1 的个数为奇数，则被认为传输正确，否则就被认为传输中出现差错。

2) 水平奇偶校验法

水平奇偶校验是以字符组为单位的一种校验方法。对一组字符中的相同位进行奇偶校验。水平奇偶校验法通常以 7 个字节(即 7 个字符)为一组，外加一个字节的校验码。

3) 水平垂直奇偶校验法

水平垂直奇偶校验是同时进行水平方向和垂直方向的奇偶校验的校验。其具体实现过程如下：

① 组成一个字符组(8 字节一个组)。

② 对每一个字符增加一个校验位(7 个数据位，1 个校验位)。

③ 对每组字符相同的位增加一个校验位(即多传输一个字节的校验信息)。

具体传输过程是,先按水平奇偶校验法进行数码传输和校验,待一组字符(8 个字节)全部传输完毕后,再进行垂直校验。

水平垂直奇偶校验法的可靠性高,但编码复杂,检测时间长。

4) 循环冗余码校验法

循环冗余检验码(Cyclic Redundancy Code,CRC)又称多项式码,它是一种在计算机网络和数据通信中用得最广泛的检错码之一。循环冗余检验码是在发送端产生一个循环冗余检验码。

循环冗余检验的基本原理如下:

设:信息码为 k 位,其多项式为($k-1$)次多项式,记为 $K(x)$。

冗余码为 n 位,其多项式为 r 次($r=n-1$)多项式,记为 $R(x)$。

由信息位产生冗余位的编码过程,就是已知 $K(x)$ 求 $R(x)$ 的过程。在 CRC 码中可以通过找到一个特定的 n 次多项式 $G(X)$,用 $G(X)$ 去除 $X^n \times K(x)$ 所得到的余式就是 $R(x)$。

例 5-2 设信息码为 1011001,冗余码为 4 位。

则有 $K(X)=X^6+X^4+X^3+1$。

说明:因信息码有 7 位,所以 $K(x)$ 为 6 次多项式,冗余码有 4 位,所以 $R(x)$ 应为 3 次多项式。

由信息位产生冗余位的编码过程,就是已知 $K(x)$ 求 $R(x)$ 的过程。在 CRC 码中可以通过找到一个特定的 n 次多项式 $G(X)$,用 $G(X)$ 去除 $X^n \times K(x)$ 所得到的余式就是 $R(x)$。

设:$K(X)=X^6+X^4+X^3+1$ 即 $K(X)=1011001$

$n=4$

$G(X)=X^4+X^3+1$ 即 11001(实际上,$G(X)$ 是 $K(X)$ 的后 5 位)

则:$X^4 \times K(X)=X^{10}+X^8+X^7+X^4$ 即 10110010000

由上看出,$X^4 \times K(X)$ 实际上是在 $K(X)$ 后添加 4 个 0 得到的。

用 $G(X)$ 去连除(即不断进行异或)$X^4 \times K(X)$ 有:

```
10110010000
11001
-----------
 1111010000
 11001
-----------
  11110000
  11001
-----------
   111000
   11001
-----------
    1010  (余数)
```

从上面演算过程中看出,经过若干次异或运算后,得到的最后余数 1010 就是所需用的冗余码 $R(X)$,记为 $R(X)=X^3+X$。

在信息接收端，用信息码与冗余码进行若干次异或运算，当余式为 0 时则认为传输无差错，否则认为传输有差错。

验算举例：设 $K(X)=1011001$，$R(X)=1010$，$G(X)=11001$

则：$T(X)=X^4\times K(X)\oplus R(X)=10110011010$

验算方法：仍然采用不断异或运算的方法进行验算，即用 $T(X)$ 与 $G(X)$ 异或，这里 $G(X)$ 取自 $K(X)$ 的后 5 位。

```
 10110011010
 11001
-------------
  1111011010
  11001
-------------
    11111010
    11001
-------------
      110010
      11001
-------------
           0
```

验算完毕。

5. 自动纠错技术

自动纠错就是在信息接收端能自动检测错误，并能进行错误编码的定位，从而能自动进行纠错。纠错很简单，将错误码求反即可，关键是如何定位错误码的位置。

1）自动校验公式及校验码

这里，以传输一个 4 位数码为例，介绍一种自动纠错的算法。

每个字符除了 4 位数码外，还要增加 4 个校验位，即一组信息共 8 位。从左到右其二进制编码用 $C1\sim C8$ 表示，其校验码计算公式如下：

$$C1\oplus C2\oplus C3\oplus C4\oplus C5=0 \qquad ①$$

$$C1\oplus C2\oplus C3\oplus C6=0 \qquad ②$$

$$C1\oplus C3\oplus C4\oplus C7=0 \qquad ③$$

$$C1\oplus C2\oplus C4\oplus C8=0 \qquad ④$$

即：

$$C5=C1\oplus C2\oplus C3\oplus C4 \qquad ⑤$$

$$C6=C4\oplus C5 \qquad ⑥$$

$$C7=C2\oplus C5 \qquad ⑦$$

$$C8=C3\oplus C5 \qquad ⑧$$

上式中，符号“$\oplus$”表示异或运算。

2）校验方法

在发送端，用⑤～⑧式计算出校验码 $C5$、$C6$、$C7$ 和 $C8$，连同前 4 位数码一起发给接收端；在接收端，用①～④式进行校验，若 4 个式子计算结果都为 0，则传输正确，只要有一个式子的计算结果为 1，则说明传输有错。

例 5-3 设信息码为1101，即 $C1=1$，$C2=1$，$C3=0$，$C4=1$，求出4位校验位 $C5$、$C6$、$C7$、$C8$。根据上述计算公式⑤～⑧计算得到：

$$C5=1\oplus 1\oplus 0\oplus 1=1$$
$$C6=1\oplus 1=0$$
$$C7=1\oplus 1=0$$
$$C8=0\oplus 1=1$$

因此，得到8位发送编码如下：

C1	C2	C3	C4	C5	C6	C7	C8
1	1	0	1	1	0	0	1

在接收端接收完8位数码后即用①～④式进行校验，若接收端收到的8位编码都正确，则4个式子的计算结果肯定为0，如果有一位错误，则到少有一个式子的结果不为0。例如设接收端收到的 $C4=0$，而其余位正确，将 $C1$～$C8$ 代入①～④，则有：

$$1\oplus 1\oplus 0\oplus 0\oplus 1=1$$
$$1\oplus 1\oplus 0\oplus 0=0$$
$$1\oplus 0\oplus 0\oplus 0=1$$
$$1\oplus 1\oplus 0\oplus 1=1$$

从上面可看出，除了②式正确（结果为0）以外，其余3式全错（结果为1）。

3）差错判断法则

- 若①、②、③、④式全错，则 $C1$ 必错。
- 若①、②、④式错而③式不错，则 $C2$ 必错。
- 若①、②、③式错而④式不错，则 $C3$ 必错。
- 若①、③、④式错而②式不错，则 $C4$ 必错。
- 若只有①式错则 $C5$ 必错。
- 若只有②式错则 $C6$ 必错。
- 若只有③式错则 $C7$ 必错。
- 若只有④式错则 $C8$ 必错。

5.3 应用实例

5.3.1 网络数据的安全传输技术

1. 网络数据传输的概念

可以说，一切通过计算机网络传输数据的过程都叫网络传输。包括在个人网络、局域网络、广域网络和国际互联网络上的数据传输。无论是接收数据，还是发送数据，只要是从一台计算机通过网络向另一台计算机传输数据，都可以理解为网络数据传输。例如，收发电子邮件、用FTP上传或下载文件、浏览网页等都属于网络数据传输。

在现代网络中,网络传输的主要协议有两个,TCP 协议和 UDP 协议。TCP 协议是面向连接的协议,可以在确认对方身份以后再进行数据交换,相对来说比较安全;而 UDP 协议是面向非连接的协议,对方在线与否都可以给对方传输数据,因 UDP 无法进行身份认证,其安全隐患比 TCP 要大得多。

2. 数据的安全传输

在网上传输数据,尤其是远程网络传输,不可避免地要经过许多称为“跳”的路由器及交换机,数据包每经过一跳,都会面临数据包被截获、被破解、被更改的危险,无论是采用面向连接的 TCP 协议还是采用面向非连接的 UDP 协议,都是如此。因此,保护网络数据正确传输的目的有两个,既要保证网络传输数据的正确性和完整性,还要对对方的身份进行认证(使用面向连接协议 TCP 时)。

对网络数据的保护通常有这样几种技术,数字签名技术与身份认证技术、数据加密技术、消息摘要技术(数据的完整性保护)和数据隐藏技术。

3. 网络数据传输法则

针对数据传输过程中的数据安全问题,HDS 公司首席安全官 Arthur B. Edmonds 给出了 5 步法则。

第 1 步是 Authentication(证明)。即证明符合所声明的身份,相关的工具包括 DABIOS、LDAP、DH-CHAP、密匙与密码等。不论何时,当建立一个数据传输通路时,这是必须要做的第一件事。这就好像是一个护照,上面记录用户所有的信息。

第 2 步是 Authorization(授权)。如果从主数据中心向次级数据中心备份数据,就需要一个长时间的通路连接。此时,次级数据中心就需要授权,即表明能做什么?被允许做什么?

第 3 步是 Audit/Accounting(稽核)。即记录用户在登录后执行过的操作。稽查日志的精度极高,它可以捕捉到每一个按键的操作。因此,用户的所有操作步骤都会被记录在日志中。

第 4 步是 Integrity(一致性)。即保证对方能够收到所发送的信息,且发送与接收的数据保持一致,而这中间也不会被其他人窜改意思。保证一致性,就是要防止黑客或其他人窃取本不该他们看到的数据。对于数据的安全性来说,这一步骤是非常重要的。

第 5 步是 Confidentiality(保密性)。即只有拥有相应权限的人才能看到保密信息,这也是通常所说的加密(encryption)。加密有软件加密和硬件加密。

通过上述 5 个步骤,就可以进行安全数据传输,最后是关闭对话通路。在这里讲述的存储安全,不仅限于从存储设备出发。安全应该建立在应用的基础上,用户需要的是一个完整的端到端的安全解决方案。不能只关心存储阵列的安全,还必须保证连接的所有设备都运行于安全协议之上。

4. 数字签名技术与身份认证技术

数字签名与身份认证技术是建立可靠性数据传输的基础,对于重要的数据,必须在

确认对方的身份后才能发送给对方。数据签名技术与身份认证技术详见 4.3.2 小节。

5. 数据加密技术

数据加密的目的是当网络传输的数据被非法截获后，非法用户无法读懂所截获的数据内容。

可采用 4.1 节介绍的任何一种数据加密技术对数据进行加密，但要注意下面两点。

- 消息摘要算法只适用于非保密通信的数据。
- RSA 算法一般只用于身份认证和对经典加密算法、DES 算法的密钥进行加密。而不提倡用于批量数据的加密。

6. 消息摘要技术

通过消息摘要，可有效地鉴别消息在传输过程中的完整性。消息摘要技术详见 4.1.6小节。

7. 信息隐藏技术

1）信息隐藏技术概述

信息隐藏（information hiding），或更严格地称为信息伪装（steganography，该单词来源于古希腊，意思是将有用或重要的信息隐藏于其他信息里面以掩饰其存在），就是将机密信息秘密地隐藏于另一非机密的信息之中。其形式可为任何一种数字媒体，如图像、声音、视频或一般的文档等。

信息隐藏将信息藏匿于一个宿主信号中，使不被觉察到或不易被注意到，且不影响宿主信号的知觉效果和使用价值。

2）信息隐藏与数据加密的区别

- 隐藏的对象不同。加密是隐藏内容，而信息隐藏主要是隐藏信息的存在性。隐藏通信比加密通信更安全，因为它隐藏了通信的发送方、接收方，以及通信过程的存在，不易引起怀疑。
- 保护的有效范围不同。传统的加密方法对内容的保护只局限在加密通信的信道中或其他加密状态下，一旦解密，则毫无保护可言；而信息隐藏不影响宿主数据的使用，只是在需要检测隐藏的那一部分数据时才进行检测，之后仍不影响其使用和隐藏信息的作用。
- 需要保护的时间长短不同。一般来说，用于版权保护的鲁棒水印要求有较长时间的保护效力。
- 对数据失真的容许程度不同。多媒体内容的版权保护和真实性鉴别往往需容忍一定程度的失真，而加密后的数据不容许一个比特的改变，否则无法脱密。

应该注意到，传统的以密码学为核心技术的信息安全和信息隐藏技术不是互相矛盾、互相竞争的技术，而是互补的。例如，将秘密信息加密之后再隐藏，是保证信息安全的最佳方案，也是更符合实际要求的方法。

3）信息隐藏技术的分类

（1）按信息隐藏技术包含的内容进行分类。

- 隐藏术（steganography）。一般指那些进行秘密通信的技术总称，通常把秘密信息嵌入或隐藏在其他不受怀疑的数据中。隐藏的方法通常假设第三方不知道隐蔽通信的存在，而且主要用于互相信任的双方进行点到点的秘密通信。因此，隐藏术一般不具有鲁棒性（“鲁棒”是 Robust 的音译，也就是健壮和强壮的意思。鲁棒性指的是在异常和危险情况下系统生存的关键。比如说，计算机软件在输入错误、磁盘故障、网络过载或有意攻击情况下，能不死机、不崩溃，就是该软件的鲁棒性）。例如，在数据改动后隐藏的信息是不能被恢复的。
- 数字水印（digital watermarking）。数字水印就是向被保护的数字对象（如静止图像、视频、音频）嵌入某些能证明版权归属或跟踪侵权行为的信息，可以是作者的序列号、公司标志、有意义的文本等。同隐藏术相反，水印中的隐藏信息具有能抵抗攻击的鲁棒性。即使知道隐藏信息的存在，对攻击者而言要毁掉嵌入的水印仍很困难。即使水印算法的原理公开也是如此。在密码学中，这就是众所周知的 Kerkhoffs 原理，加密系统在攻击者已知加密原理和算法、但不知道相应密钥时仍是安全的。鲁棒性的要求使得水印算法在宿主数据中嵌入的信息比隐藏术少。水印技术和隐藏术更多的时候是互补的技术而不是互相竞争的。
- 数据隐藏和数据嵌入（data hiding and data embedding）。通常在不同的上下文环境中，它们一般指隐藏术，或者指介于隐藏术和水印之间的应用，在这些应用中嵌入数据的存在是公开的，但没必要保护它们。例如，嵌入的数据是辅助的信息和服务，它们可以是公开得到的，与版权保护和控制存取等功能无关。
- 指纹和标签（fingerprinting and labeling）。指水印的特定用途。有关数字产品的创作者和购买者的信息作为水印而嵌入，每个水印都是一系列编码中的唯一一个编码，即水印中的信息可以唯一地确定每一个数字产品的备份，因此称它们为指纹或者标签。

（2）按不同的运行环境、载体以及所采用的算法进行分类。

随着多媒体技术和 Internet 的迅猛发展，大量重要的文件和个人信息以数字化形式存储和传输，这些信息包括文本、图像、音频以及视频等。这些都为秘密信息的隐藏提供了极好的载体，其他的一些特殊载体包括存储设备以及基于通信协议的数据包等。

- 文档文件中的信息隐藏。

早期隐藏信息的方法是用不可见的墨汁直接在纸上书写秘密信息。计算机极大地扩充了信息隐藏的空间。利用文档文件的布局就可以隐藏秘密信息。可以根据秘密信息的内容相应地调整每一行或者每个字之间的距离。还可以额外地加入空格以及不可见信息来表达秘密信息。TXT 文档、Word 文档、PDF 文档、HTML 和 XML 等各种文档中空格符以及回车符可以用来传递隐藏信息，常见的文字处理器、Web 浏览器会忽略这些空格符以及回车符，但是对这些源文件进行分析就会发现这些额外信息。

- 音频、图像和视频文件中的信息隐藏。

以图像为载体的信息隐藏方法很多，按照秘密信息的嵌入方式可以分为两类。一类

方法将秘密信息按某种算法直接叠加到图像的空间域上。考虑到视觉上的不可见性,一般是嵌入到图像中最不重要的像素位上。空间域方法的特点是计算速度快,而且很多算法不需要原始图像。

另一类方法是先将图像做某种变换(特别是正交变换),然后把秘密信息嵌入到图像的变换域中。

• 存储载体中的信息隐藏。

充分利用未用的磁盘存储空间或者保留的空间来隐藏信息不会破坏载体原有信息。操作系统在存储文件时会产生一些不用的空间。例如,在 Windows 95/98 操作系统中,FAT16 文件系统簇的大小为 32KB。这就意味着为文件分配的最小单元为 32KB。如果文件大小为 1KB,将有 31KB 的空间被浪费。这些额外的空间可以用来隐藏信息而不被正常文件系统所访问和显示。

在文件系统中另外的一种信息隐藏的方法是创建一个隐蔽分区。当正常文件系统启动时,这个分区是不可见的,但是在许多情况下,运行一些磁盘配置程序时(如 DOS 下 Fdisk)就会暴露隐蔽的磁盘分区。目前这个观点已经得到了扩充,提出了一个基于信息隐藏的文件系统。在该系统中,只有用户知道相应用户账号和口令,才可以访问该文件系统,其他用户根本不知道该文件系统是否存在。

• 网络协议数据中的信息隐藏。

网络协议有许多缺陷可以用来进行信息隐藏。例如,TCP/IP 包在因特网中传输信息,在其包头结构中有一些未用的位。在 TCP 头中有 6 个保留位,在 IP 头中有 2 个保留位。除此之外,在头结构的其他信息可以重定义来隐藏信息。比如利用包 ID 信息,TCP 握手协议的初始序列号,确认序列号隐藏信息。ICMP 包中的源抑制位同样也可以进行信息隐藏。

• 基于图灵机的信息隐藏技术。

还有一种隐藏技术,使用自动机生成一段有意义的文字。这段文字的生成是根据秘密信息的内容和自动机特定的文法实现的。

4) 信息隐藏的应用领域

(1) 隐蔽通信。

隐藏通信的收发双方,以及通信过程的存在。

(2) 版权保护。

包括确认数据的作者和数据的合法使用者(序列号)两种。这种水印属于鲁棒水印(robust watermarking)。

(3) 鉴别。

鉴别或称为“认证”,“篡改提示”,用于确认数据的真实性、完整性,提示被篡改情况。这种水印称易损水印(fragile watermarking)。

(4) 注释。

隐藏大量的信息于数据中,用于解释这些数据,如在 CD 音乐中隐藏该乐曲的简介、作曲、定购信息和访问连接等操作代码,在图像中隐藏图像名称和图像内容简介、创作者等。

这种水印要求能抵抗正常的D-A/A-D变换、噪声和一般压缩等，一般不需要抵抗恶意攻击。这种在实际应用中可能需要更高的要求，如裁剪后仍能保存保留部分的信息，甚至保留有原始数据的信息，能知道被裁剪（可能要与鲁棒水印、易损水印配合使用）。

（5）使用控制。

如DVD防复制系统，将水印信息嵌入DVD内容数据中，DVD播放机通过检测DVD数据中水印信息来判断其合法性和能否复制。

5）数字水印技术

数字水印（digital watermark）技术是在图像、声音等多媒体数据中隐藏埋入某种信息，并使其隐蔽的一种技术，隐蔽埋入的信息则称为数字水印。数字水印可以加入到没有版权保护措施的数字代码中，比如数字音乐文件、数字视频文件或数字图书等，这些数字水印代码中含有相关的版权信息，能够对数字出版物的版权起到保护作用。采用这种技术埋入的信息，人不能直接感知，只能通过数据压缩、过滤处理等方法才能检测埋入的信息。这项技术的特点是，如果他人擅自去除埋入的信息，就会严重影响音像的质量。

该项技术所具有的特点可适用数字化作品的著作权保护。因此，欧美有关厂商正积极开发采用该技术的著作权保护系统。

那么数字水印是怎样防止非法复制的呢？首先，版权所有者可在不希望被非法复制的信息内容中加入数字水印，之后通过因特网将该内容发送出，使任何人都可以自由地在服务器上公开该内容。该内容由于将数字水印作为版权信息加入到了其中，版权所有者在看到数字水印后就可以判断自己的内容是否被转载。因此，数字水印也会成为一种法律手段，数字水印将成为要求停止公开信息以及索求赔偿损失时的重要证据。

数字水印的特点是即使数据的格式发生了变化，也不会丢失。比如说，有人下载了别人公开的加入了数字水印的JPEG格式图像，并将其转换为BMP格式，数字水印的信息仍然不会丢失。这是因为数字水印并不是附加在原数据上的，而是嵌入到了原数据的本身当中，而且包含数字水印的数据看起来跟普通的数据完全一样。

5.3.2 网络死锁防范技术

当通信子网内传送的报文分组过多、结点接收速度太慢、线路容量不足时，都会导致网络性能变差，出现拥塞。当拥塞加剧就会使网络吞吐量急剧下降为零，这时网络无法工作，称为网络死锁。

其实，网络死锁就是典型的网络拥塞现象，避免网络死锁的方法有3种，缓冲区预分配法、分组丢弃法和许可证法等。

1. 缓冲区预分配法

该方法用于虚电路分组交换网中。在建立虚电路时，让呼叫请求分组途经的所有结点为虚电路预先分配一个或多个数据缓冲区。若某个结点缓冲区已被占满，则呼叫请求分组另择路由，或者返回一个“忙”信号给呼叫者。这样，通过途经的各个结点为每条虚电路开设的永久性缓冲区（直到虚电路拆除），就总能有空间来接纳并转送经过的分组。

此时的分组交换与电路交换非常相似。当结点收到一个分组并将它转发出去之后，该结点就向发送结点返回一个确认信息。该确认信息一方面表示接收结点已正确收到分组，另一方面告诉发送结点，本结点已空出缓冲区，可以接收下一个分组。

2. 分组丢弃法

该方法不必预先保留缓冲区，当缓冲区占满时，将来到的分组丢弃。若通信子网提供的是数据报服务，则用分组丢弃法来防止阻塞发生不会引起太大的影响。但若通信子网提供的是虚电路服务，则必须在某处保存被丢弃的分组的备份，以便阻塞解决后能重新传送。有两种解决被丢弃分组重发的方法，一种是让发送被丢弃分组的结点超时，使其重新发送分组直到分组被收到；另一种是让发送被丢弃分组的结点在一定次数后放弃发送，并迫使数据源结点超时而重新开始发送。但是不加分辨地随意丢弃分组也不妥当，因为一个包含确认信息的分组可以释放结点的缓冲区，若因结点无空余缓冲区来接收含确认信息的分组，这便使结点缓冲区失去了释放的机会。解决这个问题的方法可以为每条输入链路永久地保留一块缓冲区，以用于接纳并检测所有进入的分组，对于捎带确认信息的分组，在利用了所有捎带的确认释放缓冲区后，再将该分组丢弃或将该捎带好消息的分组保存在刚空出的缓冲区中。

3. 许可证法

许可证法又称定额控制法。该方法是在通信子网中设置适当数量的"许可证"的特殊信息，一部分许可证在通信子网开始工作前预先以某种策略分配给各个相关的源结点，另一部分则在通信子网工作后，允许其在网络中"漂游"。当源结点要发送来自源端系统的分组信息时，它必须首先拥有许可证，并且每发送一个分组就要注销一张许可证。目的结点方则每收到一个分组并将其递交给目的端系统后，便生成一张许可证。这样便可确保通信子网中传输的分组数量不会超过许可证的数量，从而能防止网络死锁的发生。

习　题　5

一、概念题

1. 造成网络拥塞的原因有哪些？
2. 网络拥塞控制算法有哪些？
3. 什么是噪声？噪声对通信数据有何影响？
4. 简述数据校验、数据检错、数据自动纠错的基本概念。
5. 试述计算机网络通信系统中自动请求重发、向前纠错及反馈校验法技术各自的优缺点。
6. 自动纠错技术是否可纠正所有数据传输错误？

二、计算题

1. 设信息码为“1001011”,求出其奇校验码。
2. 设信息码 $K(X)=X^6+X^3+X+1$(即 1001011),求出其校验码的冗余码 $R(X)$。
3. 设信息码为 1110,求出其 4 位自动纠错码。

第 6 章 chapter 6

局域网与 Internet 安全技术

本章从网络安全的基本概念入手，着重介绍在局域网络及 Internet 网上的实用安全技术，主要内容有局域网与广域网安全技术、无线网络安全技术、Web 安全与 IE 安全技术、电子邮件安全技术、FTP 安全技术、IPv4 及 IPv6 安全技术和 Telnet 与 DNS 安全技术。

6.1 局域网与广域网安全

6.1.1 局域网络安全

1. 局域网络安全性分析

局域网络的安全涉及多个方面，不仅有局域网本身的因素，还有来自外界的恶意破坏。其安全性主要包括 3 个方面：

- 局域网本身的安全性，如 TCP/IP 协议存在的缺陷，局域网建设不规范带来的安全隐患，或来自局域网内部的人为破坏。
- 当局域网和 Internet 连接时，受到来自外界恶意的攻击，局域网对不安全站点的访问控制。
- 建设局域网所用的媒介和设备所存在的安全问题。

2. 局域网缺陷分析

TCP/IP 协议是一组协议的总称，即 Internet 网上的协议簇，在 Internet 上，除了常用的 TCP 和 IP 协议之外，还包括其他的各种协议。应用层有传输控制协议 TCP 和用户数据报协议 UDP；网络层有 IP 和 ICMP 协议，用于负责相邻主机之间的通信。很多局域网是基于 TCP/IP 协议的，由于 TCP/IP 协议本身的不安全性，导致局域网存在如下安全方面的缺陷：

- 数据容易被窃听和截取。
- IP 地址容易被欺骗。
- 缺乏足够的安全策略。

- 局域网配置的复杂性。

3. 局域网安全技术

1）流量控制

网络必须对数据的流量加以控制，否则会发生数据碰撞和数据淹没，会引起信息丢失或者网络挂起等故障。

2）信息加密

信息加密可以采用加密软件的方法，也可采用PGP加密算法、RSA加密算法、DES加密算法或IDEA加密算法。

3）网络管理

在一个局域网中，为了保证网络安全、可靠地运行，必须要有网络管理措施。因此，需要建立网络管理中心，或者指定专人负责。其主要任务是针对网络资源、网络性能和密钥进行管理，对网络进行监视和访问控制。

4）计算机病毒的防御

计算机病毒（含计算机网络病毒）的有效预防方法是经常对系统进行病毒检查和杀毒，购买正版的杀毒软件、定期进行病毒软件的升级、及时对网络操作系统Windows 98/2000/XP打补丁。

4. 局域网安全措施

1）网络分段

网络分段是保证安全的一项重要措施，就是将非法用户与网络资源相互隔离，从而达到限制用户非法访问的目的。

网络分段可分为物理分段和逻辑分段两种方式。

- 物理分段。物理分段通常是指将网络从物理层和数据链路层（ISO/OSI模型中的第1层和第2层）上分为若干网段，各网段相互之间无法进行直接通信。目前，许多交换机都有一定的访问控制能力，可实现对网络的物理分段。
- 逻辑分段。逻辑分段是指将整个系统在网络层（ISO/OSI模型中的第3层）上进行分段。例如，对于TCP/IP网络，可把网络分成若干IP子网，各子网间必须通过路由器、路由交换机、网关或防火墙等设备进行连接，利用这些中间设备（含软件及硬件）的安全机制来控制各子网间的访问。在实际应用过程中，通常采取物理分段与逻辑分段相结合的方法来实现网络系统的安全性控制。

2）以交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是因为网络的最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（单播包）还是会被同一台集线器上的其他用户所侦听。一种很危险的情况是，用户远程登录到一台主机上，由于Telnet程序本身缺乏加密功能，用户所输入的每一个字符（包括用户名、密码等重要信息）都将被明文发送，这就给黑客提供了机会。

因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个结点之间传送，从而防止非法侦听。

3）虚拟专网

虚拟专网技术主要基于近年发展的局域网交换技术（ATM交换和以太网交换）。交换技术将传统的基于广播的局域网技术发展为面向连接的技术。因此，网管系统有能力限制局域网通信的范围而无须通过开销很大的路由器。

以太网从本质上看是广播机制，但应用了交换机和VLAN技术后，实际上转变为点到点通信。除非设置了监听口，信息交换才不会存在监听和插入（改变）问题，所以运行虚拟网技术带来的网络安全的好处是显而易见的。

6.1.2 广域网络安全

由于广域网大多采用公网来进行数据传输，信息在广域网上传输时被截取和利用的可能性就比局域网要大得多。

广域网安全解决办法主要依靠防火墙技术、入侵检测技术和网络防病毒技术。在实际的广域网安全设计中，往往采取上述三种技术相结合的方法。广域网一般采用以下安全解决方案。

1. 加密技术

加密型网络安全技术的基本思想是不依赖于网络中数据通道的安全性来实现网络系统的安全，而是通过对网络数据的加密来保障网络的安全可靠性。数据加密技术可以分为三类，即对称型加密技术（如DES算法）、非对称型加密技术（如RSA算法）和不可逆加密技术（如MD5算法）。

2. VPN技术

VPN（Virtual Private Network，虚拟专网）技术的核心是采用隧道技术，将企业专网的数据加密封装后，透过虚拟的公网隧道进行传输，从而防止敏感数据的被窃。VPN可以在Internet、服务提供商的IP、帧中继或ATM网上建立。企业通过公网建立VPN，就如同通过自己的专用网建立内部网一样，享有较高的安全性、优先性、可靠性和可管理性，同时还为移动计算提供了可能。因此，VPN技术一经推出就深得人心，VPN技术是一种很好的安全技术。

3. 身份认证技术

对于从外部拨号访问总部内部网的用户，由于使用公共电话网进行数据传输所带来的风险，必须更加严格控制其安全性。一种常见的做法是采用身份认证技术，对拨号用户的身份进行验证并记录完备的登录日志。较常用的身份认证技术，有Cisco公司提出的TACACS＋以及业界标准的RADIUS等。

6.1.3 无线局域网安全

近几年来,无线局域网发展的势头越来越猛,它接入速率高,组网灵活,在传输移动数据方面尤其具有得天独厚的优势。但是,随着无线局域网应用领域的不断拓展,其安全问题也越来越受到重视。

随着无线技术运用的日益广泛,无线网络的安全问题越来越受到人们的关注。通常网络的安全性主要体现在访问控制和数据加密两个方面。访问控制保证敏感数据只能由授权用户进行访问,而数据加密则保证发出的数据只能被所期望的用户所接收和理解。对于有线网络来说,访问控制往往以物理端口接入方式进行监控,它的数据输出通过电缆传输到特定的目的地。一般情况下,只有在物理链路遭到破坏的情况下,数据才有可能被泄漏。而无线网络的数据传输则是利用微波在空气中进行辐射传播,因此只要在 Access Point (AP)覆盖的范围内,所有的无线终端都可以接收到无线信号,AP 无法将无线信号定向到一个特定的接收设备,因此无线的安全保密问题就显得尤为突出。

目前使用最广泛的 IEEE 802.11b 标准提供了两种手段来保证 WLAN 的安全,SSID 服务配置标示符和 WEP 无线加密协议。SSID 提供低级别的访问控制,WEP 是可选的加密方案,它使用 RC4 加密算法,一方面用于防止没有正确的 WEP 密钥的非法用户接入网络,另一方面只允许具有正确的 WEP 密钥的用户才能对数据进行加密和解密。

1. 无线局域网面临的网络威胁

目前,无线网络面临的网络威胁主要有以下几个方面。

- 偷听传输的数据。可导致机密数据泄漏、曝光未保护的用户凭据、身份被盗用等。它还允许有经验的恶意用户收集与用户的 IT 系统相关的信息,然后利用这些信息攻击其他的系统或网站。
- 中途截获或修改传输数据。如果攻击者可访问无线网络,就可插入恶意计算机来中途截获、修改或延迟两个合法方的通信。
- 哄骗。无线网络的访问允许非法用户使用有效的方法来发送看似来自合法用户的数据(比如电子邮件欺骗)。
- 免费下载。入侵者利用用户的网络作为自己访问 Internet 的跳板来进行文件下载。这虽不具有太大的威胁,但会大大降低合法用户访问网络的速度与效率,而且还会降低用户可用服务的等级。
- 拒绝服务(DoS)。无线级信号干扰可通过一些简单技术(如微波炉)发出。复杂的攻击可通过低层无线协议进行,而最简单的攻击则是通过向 WLAN 发送大量的随机数据而使网络堵塞甚至瘫痪。
- 偶然威胁。某些 WLAN 功能可使无意间的攻击变得更加严重。例如,一些访问者可能在启动便携式计算机时无意间连入了用户的网络,然后就会自动连接到公司的 WLAN 上。
- 恶意 WLAN。即使用户的公司并未部署 WLAN 或已有足够的安全措施,但用户的网络仍将受到内部员工在网络中安装未授权 WLAN 的威胁。

针对上述网络威胁，最简单的对策是按表 6-1 所列出的安全防范措施。

表 6-1　无线网络安全威胁的防范措施

网络威胁	安全防范措施
偷听数据	动态分配并经常定期更改加密密钥，密钥对每个用户会话唯一，使用当前已知的方法无法恢复密钥和访问数据
截获和修改数据	由于无线客户端和无线 AP 间使用动态密钥加密，因此恶意用户无法截获或修改数据 客户端、RADIUS 服务器和无线 AP 间的相互身份验证使攻击者难以进行模拟
哄骗	安全的网络身份验证使未授权的个人无法连接网络或引入哄骗数据
免费下载	强身份验证的要求，禁止未授权的网络使用
DoS	安全访问控制可禁止网络层的数据泛滥攻击，但当前没有预防低层 DoS 攻击的方法。该问题将由 2004 年的 802.11i 标准解决。在更基本的层面上，即使该标准也将受到无线网络干扰 值得注意的是，多数已发布的 DoS 攻击不会引起服务的持续丢失，DoS 攻击源一旦消失，服务立即恢复正常状态。从这种意义上讲，阻止网络层 DoS 攻击是重要的措施
偶然威胁	要求安全身份验证的 WLAN 将消除非授权用户偶然接入公司 WLAN 所带来的威胁
恶意 WLAN	尽管本解决方案并未直接处理恶意无线 AP，但通过实施安全无线解决方案（如本方案），设置非正式 WLAN 的驱动因素大大减少 通过使用扫描网络无线 AP 硬件地址的软件工具和手提的 WLAN 检测设备，恶意 WLAN 的问题也得到了解决

2. 无线局域网的安全技术

1）扩展频谱技术

扩展频谱技术在 20 世纪 50 年代第一次被军方公开介绍，它用来进行保密传输。从一开始它就设计成抗噪音、干扰、阻塞和未授权检测。扩展频谱发送器用一个非常弱的功率信号在一个很宽的频率范围内发射出去，与窄带射频相反，它将所有的能量集中到一个单一的射频点。

2）用户认证：口令控制技术

为了无线网络的安全，在无线网的站点上必须使用口令控制技术，诸如 Novell NetWare 和 Microsoft NT 等网络操作系统和服务器提供了包括口令管理在内的内建多级安全服务。口令应处于严格的控制之下并经常予以变更。由于无线局域网的用户包括移动用户，而移动用户倾向于把笔记本计算机移来移去，因此，严格的口令策略等于增加了一个安全级别，有助于确认网站是否正被合法的用户使用。

3）数据加密

假如用户的数据要求极高的安全性，需要采取一些特殊的措施。最高级别的安全措

施就是在网络上整体使用加密产品。数据包中的数据在发送到局域网之前要用软件或硬件的方法进行加密。只有那些拥有正确密钥的站点才可以恢复和读取这些数据。网络操作系统本身具有加密能力,但基于每个用户或服务器、价位较低的第三方加密产品也可以胜任,比如 McAfeeAssicoate 的 NetCrypto 或 Captial Resour-ces Snare 等加密产品能够确保唯有授权用户可以进入网络、读取数据。鉴于第三方加密软件开发商致力于加密事务,并可为用户提供最好的性能、质量服务和技术支持。

4)基于 802.11 的安全

本方法根据共享密钥和 LAN 网卡硬件地址利用无线传输的 WEP 加密和可选的网络访问控制。

5)使用 VPN 技术

使用 VPN 技术保护 WLAN 传输已成为高安全环境中一种广受欢迎的方法。它依赖于 VPN 应用程序固有的访问控制和加密。

6)使用 IPSec 安全

IPSec 是一种安全验证身份并加密网络 IP 数据包的解决方案。很多 VPN 解决方案使用 IPSec,但此处 IPSec 的使用在单个网络范围内,用以确保两台计算机之间进行端对端传输的安全。尽管 IPSec 不是网络硬件层实施的原 WLAN 保护措施的直接替代,但它和 VPN 一样在很多情况下是极佳的解决方案。

7)关闭网络接入点

无线接入点安全的关键是禁止非授权用户访问网络,也就是说,安全的接入点对非授权用户是关闭的。保障无线网络的安全比保障有线网络的安全要困难得多。因为有线网络只有有限个固定的接入点,而无线网络可以从天线允许范围内的任意一点接入。

8)设计天线的放置位置

使无线接入点保持封闭的第一步是正确放置天线,从而限制能够到达天线有效范围的信号量。不要把天线放在靠近窗户的地方,因为玻璃不能阻挡无线信号。天线的理想位置是目标覆盖区域的中心,并使泄露到墙外的信号尽可能的少。不过,完全控制无线信号是几乎不可能的,所以还需要同时采取其他一些措施来保证网络安全。

9)改变服务集标识符并且禁止 SSID 广播

服务集标识符(SSID)是无线接入的身份标识符,用户用它来建立与接入点之间的连接。这个身份标识符是由通信设备制造商设置的,并且每个厂商都用自己的默认值。例如,3COM 的设备都用 101。因此,知道这些标识符的黑客可以很容易不经过授权就享受用户的无线服务。需要给每个无线接入点设置一个唯一并且难以推测的 SSID。

如果可能的话,还应该禁止用户的 SSID 向外广播。这样,用户的无线网络就不能通过广播的方式来吸纳更多用户,当然这并不是说用户的网络不可用,只是它不会出现在可使用网络的名单中。

10)禁用动态主机配置协议

通过这个策略,将迫使黑客去破解用户的 IP 地址、子网掩码以及其他的 TCP/IP 参数。黑客想接入用户的无线网络,必须花很长的时间去破获用户的 IP 地址。

11）禁用或修改 SNMP 设置

如果用户的无线接入点支持 SNMP，那么需要禁用它或者修改默认的公共和私有的标识符。如果不这么做，黑客将可利用 SNMP 获取用户网络的重要信息。

12）使用访问列表

为了更好地保护用户的网络，尽可能设置一个访问列表。但是，不是所有的无线接入点都支持这一功能。如果能够这样做的话，就可以指定某台机器有权访问接入点。支持这项功能的接入点有时利用 TFTP（简单文件传输协议）定期地来下载更新访问列表，从而避免了必须使所有设备上的列表保持同步的巨大管理麻烦。

13）访问控制，利用 ESSID、MAC 限制，防止非法无线设备入侵

为了提高无线网络的安全性，在 IEEE 802.11b 协议中包含了一些基本的安全措施，包括无线网络设备的服务区域认证 ID（ESSID）、MAC 地址访问控制以及 WEP 加密等技术。IEEE 802.11b 利用设置无线终端访问的 ESSID 来限制非法接入。在每一个 AP 内都会设置一个服务区域认证 ID，每当无线终端设备要连上 AP 时，AP 会检查其 ESSID 是否与自己的 ID 一致，只有当 AP 和无线终端的 ESSID 相匹配时，AP 才接受无线终端的访问并提供网络服务，如果不符就拒绝给予服务。利用 ESSID，可以很好地进行用户群体分组，避免任意漫游带来的安全和访问性能的问题。

另一种限制访问的方法就是限制接入终端的 MAC 地址以确保只有经过注册的设备才可以接入无线网络。由于每一块无线网卡拥有唯一的 MAC 地址，在 AP 内部可以建立一张“MAC 地址控制表”，只有在表中列出的 MAC 才是合法可以连接的无线网卡，否则将会被拒绝连接。MAC 地址控制可以有效地防止未经过授权的用户侵入无线网络。

14）数据加密，基于 WEP 的安全解决方案

无线网络安全的数据加密可以通过 WEP（Wired Equivalent Privacy）协议来进行。WEP 是 IEEE 802.11b 协议中最基本的无线安全加密措施。WEP 是所有经过 WiFiTM 认证的无线局域网络产品所支持的一项标准功能，由国际电子与电气工程师协会（IEEE）制定，其主要用途如下：

- 提供接入控制，防止未授权用户访问网络。
- WEP 加密算法对数据进行加密，防止数据被攻击者窃听。
- 防止数据被攻击者中途恶意篡改或伪造。

WEP 加密采用静态的保密密钥，各 WLAN 终端使用相同的密钥访问无线网络。WEP 也提供认证功能，当加密机制功能启用，客户端要尝试连接上 AP 时，AP 会发出“Challenge Packet”给客户端，客户端再利用共享密钥将此值加密后送回存取点以进行认证比对，如果正确无误，才能获准存取网络的资源。AboveCable 所有型号的 AP 都支持 64 位或（与）128 位的静态 WEP 加密，能有效地防止数据被窃听盗用。

利用 128 位 WEP 加密，使得数据在无线发射之前进行复杂的编码处理，在接受之后通过反向处理获取原数据。这种加密方式确保数据的安全，即使数据泄露出去，也不会暴露数据的原值。

由于 WEP 密钥必须通过人工手动设置，因此 AboveCable 建议在无线覆盖范围不能

太大，终端用户数量不能太多，且对安全要求不是很高的应用环境下使用该技术是最经济最方便的。

无线安全技术特别适合一些小型企业、家庭用户等小型环境的无线网络应用，无需额外的设备支出，配置方便，且安全防护性好，从终端的访问控制到数据链路中的数据加密都定义了有效的解决方案。有了这些技术，用户可以快速地建立起一个安全的无线网络环境，即节约了成本又可达到预计的安全目标，使无线网络的使用价值大大提高。

15）新一代无线安全技术——IEEE 802.11i

在某些场合，如大型企业、银行、证券行业，其现有的网络结构比较复杂且对网络的安全性要求很高，仅使用基本的安全措施并不能完全达到其安全需求。为了进一步加强无线网络的安全性，IEEE 802.11 工作组目前正在开发作为新的安全标准的 IEEE 802.11i，并且致力于从长远角度考虑解决 IEEE 802.11 无线局域网的安全问题。IEEE 802.11i 标准草案中主要包含加密技术 TKIP（Temporal Key Integrity Protocol）和 AES（Advanced Encryption Standard），以及认证协议 IEEE 802.1x。

16）端口访问控制技术（IEEE 802.1x）和可扩展认证协议（EAP）

IEEE 802.1x 是一种基于端口的网络接入控制技术，在网络设备的物理接入级对接入设备进行认证和控制。IEEE 802.1x 可以提供一个可靠的用户认证和密钥分发的框架，可以控制用户只有在认证通过以后才能连接网络。IEEE 802.1x 本身并不提供实际的认证机制，需要和上层认证协议（EAP）配合来实现用户认证和密钥分发。EAP 允许无线终端可以支持不同的认证类型，能与后台不同的认证服务器进行通信，如远程接入用户服务（RADIUS）。

17）综合使用无线和有线策略

无线网络安全不是单独的网络架构，它需要各种不同的程序和协议配合。制定综合利用有线和无线网络安全的策略能够极大地提高安全水平。

6.1.4 网络安全体系结构

1. OSI 安全模型

ISO/OSI 模型共分为 7 个层次，作为网络安全体系，是贯穿于整个 7 层模型中的，如图 6-1 所示。

2. OSI 分层安全机制

OSI 模型是分层次的，图 6-1 就是 OSI 层次模型中各层提供的安全功能和网络所采取的对应措施。

1）物理层安全

物理层的信息安全主要是防止物理通路的损坏、物理通路的窃取以及对物理通路的攻击等。换句话说，物理层的安全有连接的机密性服务、通信业务流机密性服务等。其具体的实现技术是数据加密和通信业务流填充机制。

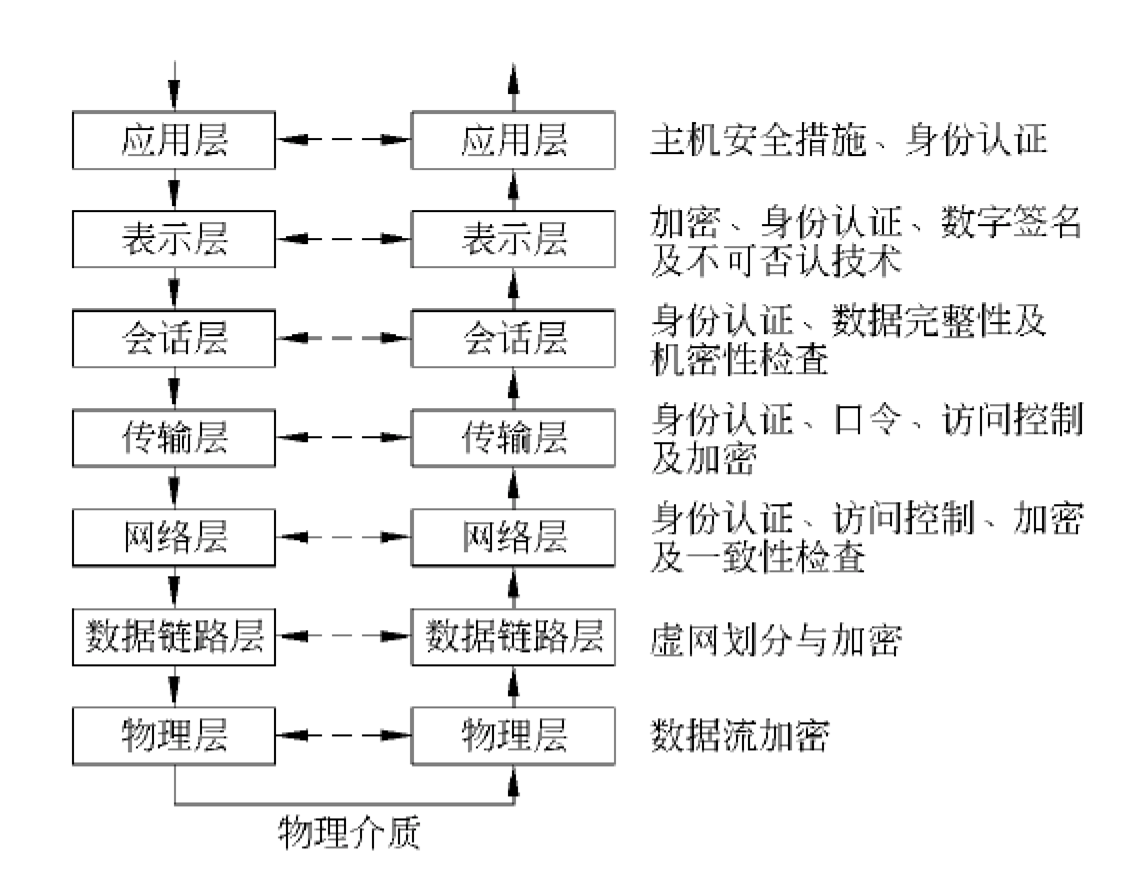


图 6-1　OSI 安全模型

2）数据链路层安全

数据链路层的安全需要保证通过网络链路传送的数据不被窃听，支持面向连接的服务和面向不连接的服务。通常可采用划分虚网和加密通信等手段。

3）网络层安全

网络层的安全需要保证网络只给授权的客户使用授权服务，保证网络路由正确，避免被拦截或被监听。具体的安全服务技术有对等实体鉴别、数据原发鉴别、访问控制鉴别、连接机密性、无连接的机密性和通信业务流机密性等。

4）传输层安全

传输层可提供的安全服务有对等实体鉴别、数据原发鉴别、访问控制鉴别、连接机密性和无连接的机密性等。

5）会话层安全

会话层提供安全服务主要有会话连接的数字签名技术及身份认证技术。

6）表示层安全

表示层将支持经应用层向应用进程提供的安全服务，连接机密性、无连接的机密性、通信业务流机密性、对等实体鉴别、数据原发鉴别、数据原发证明的抗抵赖性以及交付证明的抗抵赖性等。

7）应用层安全

应用层提供的是面向所有应用进程、应用端口的安全。原则上说，应用层的安全包含了所有低 6 层的安全。

8）操作系统安全

操作系统的安全主要要保证客户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

9）应用平台安全

应用平台指的是建立在网络之上的应用软件服务，如数据库服务、电子邮件服务、

Web 服务器等。由于应用平台的系统非常复杂，通常可采用多种技术来增强应用平台的安全性。例如 SSL(Secure Socket Layer，安全套接字层)服务。

10) 应用系统安全

应用系统的最终目的是为用户服务。因此，应用系统的安全与系统设计和实现关系密切。应用系统使用应用平台提供的安全服务来保证其安全，如通信安全、通信双方的认证和审计手段等。

ISO/OSI 模型的分层安全机制如表 6-2 所示。

表 6-2 ISO/OSI 模型的分层安全机制

OSI 层	安全机制	OSI 层	安全机制
应用系统	应用系统安全	网络层	安全路由/访问机制
应用平台	应用平台安全	数据链路层	数据链路安全
操作系统	操作系统安全	物理层	物理层信息安全

3. 网络安全体系及实现技术

计算机网络安全体系结构由网络安全性、系统安全性、用户安全性、应用程序安全性以及数据安全性等 5 个层面组成，其对应的实现技术如表 6-3 所示。

表 6-3 网络安全体系结构及实现技术

安全层次	安全内容	安全实现技术
数据安全性	保证数据的安全	密码技术
应用程序安全性	应用程序对数据的合法访问权限和对用户的合法访问权限	访问控制技术和身份认证技术
用户安全性	防止非法用户使用网络	分组管理技术、身份认证技术
系统安全性	保证客户资料、操作系统访问控制的安全，防止计算机病毒和黑客对网络的侵入和破坏	访问控制技术
网络安全性	防止数据外泄、保证数据传输的安全	防火墙技术和 VPN(虚拟专用网络)技术

6.2 Internet 安全

6.2.1 Internet 网络体系结构

Internet 网络是基于 TCP/IP 协议的，TCP/IP 协议又称为 TCP/IP 模型，是国际互联网 Internet 的协议簇，也是一种分层结构，共分为 4 层，网络接口层、互联网层、传输层和应用层。其中网络接口层对应于 OSI 模型的第 1 层和第 2 层，互联网层对应于 OSI 模

型的第 3 层，传输层对应于 OSI 模型的第 4 层，应用层对应于 OSI 模型的第 5 层、第 6 层和第 7 层，如图 6-2 所示。

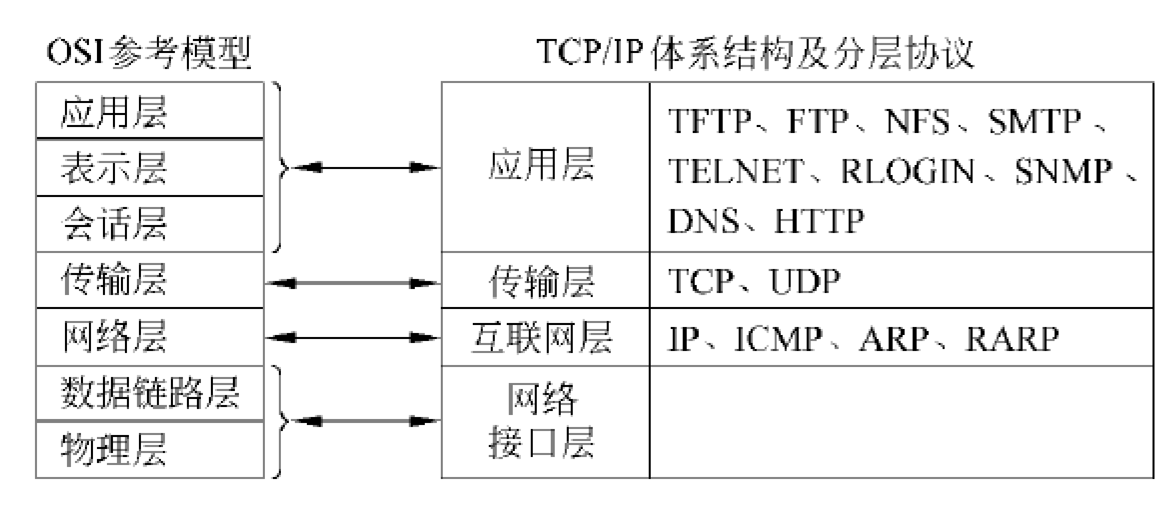


图 6-2 OSI 参考模型与 TCP/IP 协议对应关系

6.2.2 TCP/IP 安全性分析

TCP/IP 的层次不同提供的安全性也不同，例如，在网络层提供虚拟私用网络，在传输层提供安全套接服务。下面将分别介绍 TCP/IP 不同层次的安全性和提高各层安全性的方法。

协议模型网络安全贯穿于信息系统的 4 个层次，即网络接口层、网络层、传输层和应用层。为此基于 TCP/IP 分层模型的网络安全服务也是分层的，相应的不同层次的网络服务也是不同的，需要分层进行配置。表 6-4 是 TCP/IP 分层模型中提供的网络安全服务。

表 6-4 TCP/IP 分层模型中提供的网络安全服务

服　务	TCP/IP 协议			
	网络接口层	互联网层	传输层	应用层
对等实体鉴别		Y	Y	Y
数据源发鉴别		Y	Y	Y
访问控制服务		Y	Y	Y
机密性连接	Y	Y	Y	Y
非机密性连接	Y	Y	Y	Y
选择字段机密性				Y
通信业务流机密性	Y	Y		Y
带恢复的连接完整性			Y	Y
不带恢复的连接的完整性		Y	Y	Y
选择字段连接完整性				Y
无连接完整性		Y	Y	Y
选择字段无连接完整性				Y
抗否认				Y

Y——表示具有对应的功能。

1. 网络接口层安全

网络接口层是TCP/IP的最低层，包括OSI的物理层、数据链路层。网络接口层有两种类型：第一种是设备驱动程序（如局域网的网络接口），第二种是包含自身数据链路协议的复杂子系统（如X.25中的网络接口）。为保证通过网络链路传送的数据不被窃听，主要采用划分VLAN、加密通信（远程网）等手段进行加密。

对于通过使用VPN业务连接多个私有地点的组织应该使用NAT、防火墙和数据加密技术。在VPN拓扑结构中，私有数据在公共网络上传送，因此加密是必须的。第2层隧道协议（L2TP）就是互联网工程任务组（IETF）针对在公共网络上用隧道传送私有数据而制定的标准。作为VPN业务中的一种，光虚拟专用网（OVPN）是下一代光传送网“智能光网络”最有潜力的增值业务。OVPN的关键技术包括安全隧道与信息加密技术，即使用加密与封装相结合的技术对用户数据进行安全保护；在VPN用户访问网络资源及管理员对VPN系统进行管理之前，采用用户认证技术进行身份认证；访问控制技术提供细粒度的访问控制功能以实现对用户信息资源的保护。

使用光虚拟专用网不仅具有共享的经济性、灵活性、可靠性和可扩展性等特点，更重要的是它在光层的安全性受到电信运营商的重视，这对于客户来说费用支出更少，而对于运营商来说则有更多的收入、更安全的网络。可以说，OVPN服务对于用户和运营商来说是一种双赢的选择方案，在将来的智能光网络领域有着广泛的应用前景。

2. 互联网层安全

网络层安全即IP层安全性，它的主要优点是其透明性，也就是说，安全服务的提供不需要应用程序，也不需要对其他通信层次和网络部件做任何改动。最主要的缺点是IP层一般对属于不同进程的包不作区别。对所有去往同一地址的包，它将按照同样的加密密钥和访问控制策略来处理，这将使得网络安全性能下降。针对面向主机密钥分配的问题，RFC 1825推荐使用面向用户的密钥分配，其中，不同的连接会得到不同的加密密钥。然而，面向用户的密钥分配需要对相应的操作系统内核作比较大的改动。

IP层非常适合提供基于主机的安全服务，相应的安全协议可以用来在互联网上建立安全的IP通道和虚拟专网。例如，利用它对IP包的加密和解密功能，可以简捷地强化防火墙系统的防卫能力。

网络层的安全性问题核心在于网络是否能得到控制，目标网站通过对源IP进行分析，便能够初步判断来自这一IP的数据是否安全，是否会对本网络系统造成危害，来自这一IP的用户是否有权使用本网络的数据。一旦发现某些数据来自不可信任的IP地址，系统便会自动将来访者阻挡在系统之外，并且大多数系统能够自动记录那些曾经造成过危害的IP地址，使它们的数据无法造成第二次危害。网络层主要的安全技术包括防火墙技术、IPSec技术、端口扫描技术及入侵检测技术。

3. 传输层安全

传输层的脆弱性已经成为网络协议攻击的主要突破口之一，其漏洞如下：

- TCP 连接的建立与终止。TCP 连接的建立与断开机制保证了传输的可靠性与速度,但是在连接建立过程完成之后,服务器端不再验证连接的另一方是不是合法的用户,这种脆弱性的直接后果是连接可能被窃取。
- TCP 连接请求对队列的处理方法看起来很适用于连接的实际情况,但是很容易出现以下现象:如果某一用户不断地向服务器某一端口发送申请 TCP 连接的 SYN 请求包,但不对服务器的 SYN 包发回 ACK 确认信息,则无法完成连接。当未完成的连接填满传输层的队列时,它不再接受任何连接请求,包括合法的连接请求,这样就可能使服务器端口服务挂起。
- TCP 连接的保持。TCP 连接仍旧能保持的特性会造成当 TCP 连接上很长时间内无数据被传送时 TCP 连接资源的浪费。毕竟服务器某个端口可以存在的最大连接数有限,保持着大量不传输数据的连接将极大地降低服务器性能,而且在服务器的两次探测之间,可能导致 TCP 连接被窃取,使得原来与服务器连接的机器死机或重启。

由于 TCP/IP 协议本身非常简单,没有加密、身份认证等安全特性,因此要向上层应用提供安全通信的机制就必须在 TCP 之上建立一个安全通信层次。传输层网关就是在两个通信结点之间代为传递 TCP 连接并进行控制,这个层次一般称作传输层安全。同网络层安全机制相比,传输层安全机制的主要优点是它提供基于进程对进程(而不是主机对主机)的安全服务和加密传输信道,利用公钥体系进行身份认证,是一种安全强度高、支持用户选择的加密技术。如果再加上应用级的安全服务,就可以提供更加安全可靠的安全性能。

4. 应用层安全

应用层的缺陷主要集中在 R 系列命令中(rcp、rsh、rlogin 等),这些命令是基于可信任主机之间的关系而设置的方便用户登录的方法,可信任主机不需要口令也可以通过 R 系列命令登录进入目标系统。

在应用层提供安全服务有,首先是对每个应用分别进行修改和扩展,加入新的安全功能。例如,在 RFC1421～1424 中,IETF 规定了私有强化邮件(PEM)为基于 SMTP 的电子邮件系统提供安全服务,应用层对防止系统遭病毒侵入和黑客攻击都有极其重要的作用。另外,应用层还可以使用应用平台提供的安全服务,如采用通信内容安全保护、通信双方的认证、审计等手段来保证基本安全。

在安全性设计中包含的任务与网络总体设计所包含的任务是一致的,分析网络安全需求和目标,对其复杂性作出折中,因为任何网络没有绝对的安全,安全的保护和策略越复杂,则投入的网络运营成本越高。因此,较理想的安全机制是找到两者的平衡点,制定出一种合适的安全策略。

6.2.3 Internet 存在的安全漏洞

1. 安全漏洞

1) 安全漏洞

安全漏洞是指任意允许非法用户未经授权获得访问或提高访问层次的硬件和软件。

1977年，为了改善不同制造商生产的系统之间的通信，国际标准化组织(ISO)开发了开放系统互连参考模型(OSI)。在OSI的每一层，数据存在的方式和遵守的协议各不相同。其中TCP/IP(传输控制协议和网际协议)和UDP(用户数据报协议)是该模型的基本协议，而这些协议在开始制定时就没有考虑通信路径的安全性，从而导致了网络上的远程用户读、写系统文件或执行根和非根拥有的文件并通过网络进行传送、跨越防火墙读或写系统文件等安全漏洞。从纯技术的角度上说，缺乏安全防护设备与管理系统、缺乏通信协议的基本安全机制、基于HTTP与FTP上的应用软件问题以及不够完善的服务程序等也是产生安全漏洞的主要原因。

2）常见的黑客攻击点

黑客进行网络攻击主要寻找计算机固有的安全漏洞，常从以下几个方面进行攻击。

（1）身份认证和访问控制管理部分。

黑客能够成功入侵网络的主要原因是身份认证和访问控制机制不够完备。所有身份认证系统的核心是检查用户身份并判定用户具有何种访问权限，而能否得到用户的口令是黑客入侵成败的关键。黑客常采用猜测、利用一些口令软件、采用嗅探程序滤出口令、利用TSR驻留程序监视用户登录等办法获取口令。Internet上的许多黑客站点可以免费下载一些刺探软件，为黑客入侵提供了方便。所以用户在选择口令时，不要图简单易记而忽略了设定口令应该遵守的基本规则。

（2）通信协议部分。

TCP/IP协议簇是所有协议的基础。在发送信息时常包含源地址、目标地址和端口号等信息，所以TCP协议、IP协议和UDP协议成为黑客攻击的主要目标。利用这些协议自身存在的隐患进行攻击的手段很多，主要包括IP地址欺骗(IP spoofing)、IP碎片袭击、TCP序号攻击和UDP欺骗等。

（3）应用软件部分。

OSI模型的应用层管理访问远程系统所提供服务的程序请求，它包括FTP、NFS和TFTP等文件传输服务、远程登录应用(Telnet、rsh、rcp和rlogin)服务和电子邮件(SMTP)服务、Internet新闻服务(NNTP)以及网络管理服务(SNMP)等，而这些服务都以IP、TCP和UDP协议为基础。如果管理不当，Internet实现的这些服务也会带来安全隐患。这些服务应遵守仅完成所请求服务的原则，避免给系统带来不必要的损失。

（4）网络服务器部分。

随着多媒体技术的发展，人们由网络上的静态文本需求转化为视频、音频及图像等多媒体需求，20世纪90年代引入的Web服务器与Internet Explorer和Netscape等浏览器的结合基本满足了这一要求。Web是一个基于Internet/Intranet的、全球连接的、分布的、动态的和多平台的交互式超媒体信息系统，它经历了静态文档、动态交互界面和电子商务3个重要阶段。Web浏览器和Web服务器之间遵守HTTP协议。它与绝大多数服务不同，在用户从Web服务器上检索信息的时候，它不生成和维护一个单独的会话。一个带有许多图形的Web页面需要生成多个同时运行的连接才能装入浏览器中，Web浏览器常常为了读取一个Web页面生成几十个会话，这就为黑客窃听和截取信息提供了可乘之机。

另外,Gopher 也是一种功能强大、结构简单的文件检索工具。Gopher 服务器可以彼此连接起来,用户可以透明地在多个系统上检索文件信息,Gopher 客户和 Gopher 服务器之间遵守 Gopher 协议。由于 Gopher 和 Web 服务器的软件结构庞大而且复杂,存在着许多安全隐患,HTTP 协议和 Gopher 协议不适合传递保密信息,而 SHTTP 协议和 SSL 协议则解决了保密信息的传输问题。

许多网络服务器使用的是 UNIX 操作系统,基于该操作系统的网络模块都是从 BSD(伯克利大学系统分发版本)的 UNIX 系统中的网络代码派生出来的,而 BSD 系统的网络部门的代码流传较广,攻击者通过对其分析就能发现部分网络模块中的缺陷,从而找到访问系统的攻击点。

2. 常用防范措施及其缺陷

针对上述的安全漏洞,通常采用路由器技术和防火墙技术进行防范。

1)路由器技术

路由器是一种多端口设备,在网络上按照协议对数据帧进行转发。路由器位于一个或多个网段的交界处,它工作在网络层和传输层。在网络层,当路由器遇到一个 IP 包时,它便检查 IP 包中的目的 IP 地址,并与路由选择表中的项目进行比较。如果匹配,路由器则依照表中的指示转发 IP 包,如果不匹配,且没有默认的路由选择,IP 包便被滤掉。在传输层,路由器利用 TCP 报头中的源端口号、目的端口号和 TCP 标志(如 SYN 和 ACK 标志)进行包过滤。路由器可以阻塞广播信息和不知名地址的传输,达到保护内部安全的目的。

路由器只在 IP 和 TCP 层工作,而 IP 层和 TCP 层与应用层的问题毫不相关,但是由于它考虑的只是 IP 层和 TCP 层的地址、端口号和 TCP 标志等信息作为判定过滤与否的唯一依据,并没有对其他安全需求做出说明,因此路由器不能对通过高层协议进行的攻击实现有效的检测。另外,对于一些协议如 UDP(没有 TCP 标志位 ACK)和远程程序调用(RPC)很难进行过滤。路由器防范入侵的主要措施就是根据系统要求确定路由规则,设计包过滤访问列表(ACL),能否达到安全要求取决于对通信协议及行为的理解。

在许多包过滤器的实现中,过滤规则的数量也受到一定限制。随着规则数目的提高,需要额外的方法对附加规则进行处理,因此相应的成本也会提高。路由器的另一个缺点是在许多包过滤实施中缺乏审计和报警装置。

总之,多数路由器采用静态分组过滤来控制网络信息传输,它适用于对安全要求不是很高的场合。实际应用中一般与防火墙结合使用,从而达到更加安全的效果。

2)防火墙技术

目前保护网络安全最主要的手段之一是构筑防火墙,它一般位于开放的、不安全的公共网与内部局域网之间,用于实现两个网络之间的访问控制和安全防范。防火墙技术详见第 8 章。

3. Web 面临的安全威胁

Web 服务所面临的安全威胁可归纳为两种,一种是机密信息所面临的安全威胁,另

一种是WWW服务器和浏览器主机所面临的安全威胁。其中,前一种安全威胁是Internet上各种服务所共有的,而后一种威胁则是由扩展Web服务的某些软件所带来的。这两种安全隐患也不是截然分开的,而是共同存在并相互作用的,尤其是后一种安全威胁的存在,使得保护机密信息的安全更加困难。

4. WWW服务器和浏览器主机所面临的安全威胁

1) CGI通用网关程序所带来的威胁

CGI是英文Common Gateway Interface(通用网关接口)的缩写,它在服务器端与Web服务器相互配合,响应远程用户的交互性请求。它允许用户选择一种语言,如C/C++、Perl、UNIX Shell、VB等进行编程,提供在服务器端和远程浏览之间的信息交互能力。

CGI Script是Web安全漏洞的主要来源。其安全漏洞存在于以下3个方面。

- 会泄露主机系统的信息,容易导致黑客入侵。
- 当服务器处理远程用户输入的某些信息(如表格)时,易被远程用户攻击。
- 不规范的第三方CGI程序,或存有恶意的客户发布给Web服务器的CGI程序,会对Web服务器造成物理或逻辑上的损坏,甚至将Web服务器上的整个硬盘信息复制到Internet的某一台主机上。

2) Java小程序所带来的威胁

Java是由美国Sun Microsystems公司于1995年推出的一种跨平台和具有交互能力的计算机程序语言,具有简单、面向对象、分布式、健壮、安全、结构中立、可移植、高效、多线程和动态等优点。Java小程序由浏览器进行解释并在客户端执行,因此把安全风险直接从服务器端转移到了客户端。

尽管在实现Java小程序时进行了很多安全方面的考虑,但在发行后的很短时间内,在Java中就发现了很多由于具体实现的Bug而引起的安全漏洞。

在Netscape 2.0中Java的实现中存在一些特殊的安全漏洞,例如任意执行机器指令的能力、Applet(小程序)的相互竞争力和与随意的主机建立连接的能力。

此外,Java Script作为Java Applet在IE、NetScape中的实现语言,还存在着以下一些安全漏洞。

- 可以欺骗用户,会将本地硬盘或连在网络上的磁盘上的文件传输到Internet上的任意主机。
- 能获得用户本地硬盘和任何网络盘上的目录列表。
- 能监视用户某段时间内访问过的所有网页,捕捉URL并将它们传送到Internet上的某台主机中。
- 能够不经用户允许而触发NetScape Navigator发送出E-mail信息。

3) ActiveX控件所带来的威胁

ActiveX是微软在其组件对象模型(component object model)之上建立的一种理论和概念,同时也是一种新的编程标准,可以用任何一种面向对象的语言加以实现,如VC、VB等,用这种规范建立起来的ActiveX控件真正实现了多语言编程的无缝连接,同时,

这种控件也可以嵌入 HTML 文本中，形成一定功能的程序模块。

由于 ActiveX 控件被嵌入到 HTML 页面中，并下载浏览器端加以执行，因此会给浏览器端造成一定程度的安全威胁。此外，目前已有证据表明，在客户端的浏览器中，如在 IE 中插入某些 ActiveX 控件，也将直接对服务器端造成意想不到的安全威胁。

另外，内嵌于 IE 的 VB Script 语言，用这种语言生成的客户端可执行的程序模块，也同 Java 小程序一样，有可能给客户端带来安全性能上的漏洞。此外，还有一些新技术，如 ASP(Active Server Pages)技术，由于用户可以为 ASP 的输出随意增加客户脚本、ActiveX 控件和动态 HTML，因此在 ASP 脚本中同样也都存在着一定的安全隐患。

6.3 Web 安全与 IE 安全

6.3.1 Web 安全漏洞分析

1. Web 漏洞

典型的 Web 漏洞如下：

- 操作系统的安全漏洞。比如由于操作系统本身的漏洞，使得未授权的用户可以获得 Web 服务器上的秘密文件、目录或重要数据。
- 明文或弱口令漏洞。当远程用户向服务器发送信息时，特别是信用卡之类，中途可能会被网络攻击者非法拦截。如果客户和服务器间的通信是明文或弱口令加密方式，并且传输的信息是明文形式，一切都会暴露；或者虽然经过加密，但加密的口令仍是弱口令，密文仍然可能会被网络攻击者解密。
- Web 服务器本身存在的一些漏洞，使得非法用户能侵入到主机系统破坏重要的数据，甚至造成系统瘫痪。
- CGI 安全方面的漏洞。用 CGI 脚本编写的程序当涉及到远程用户从浏览器中输入表格(form) 并进行检索(search index)或 Form-mail 之类在主机上直接操作命令时，会给 Web 主机系统造成危险。因此，从 CGI 角度考虑 Web 的安全性，主要是在编制程序时，应详细考虑到安全因素，尽量避免 CGI 程序中存在漏洞。

2. Web 服务器版本漏洞分析

早期版本的 HTTP 存在明显的安全漏洞，即客户计算机可以任意地执行服务器上面的命令，现在的 Web 服务器已弥补了这个漏洞。

因此，不管是配置服务器，还是在编写 CGI 程序时都要注意系统的安全性。尽量堵住任何存在的漏洞，创造安全的环境。在具体服务器设置及编写 CGI 程序时应该注意以下几点。

- 禁止乱用从其他网站下载的工具软件，并在没有详细了解之前尽量不要用 root 身份注册，以防止程序中设下的陷阱。
- 在选用 Web 服务器时，应考虑到不同服务器对安全的要求不一样。某些简单的

Web 服务器就没有考虑到安全的因素,不能把他用作商业应用,只作一些个人的网点。

- 注意,在利用 Web 中的“.htpass”来管理和校验用户口令时,存在校验的口令和用户名不受次数限制。

6.3.2 Web 服务器安全性分析

1. Web 欺骗

Web 欺骗允许攻击者将对一个正常 Web 访问流量全部引入到另一个攻击者的 Web 服务器,经过攻击者机器的过滤作用,允许攻击者监控受攻击者的任何活动,包括账户和口令。攻击者也能以受攻击者的名义将错误或者易于误解的数据发送到真正的 Web 服务器,并能以任何 Web 服务器的名义发送数据给受攻击者。简而言之,攻击者观察和控制着受攻击者在 Web 上做的每一件事。

2. Web 服务器安全预防措施

对 Web 服务器有下面的安全预防措施。

- 对在 Web 服务器上新开的账户,在口令长度及定期更改方面作出要求,防止被盗用。
- 尽量使 FTP,Mail 等服务器与 Web 服务器分开,关掉 FTP、Sendmail、TFTP、NIS、NFS、Finger、Netstat 等一些无关的服务。
- 在 Web 服务器上删除一些绝对不用的 shell 之类解释器,如果在 CGI 程序中没用到 perl 时,就尽量把 perl 从系统解释器中删除。
- 定期查看服务器中的日志 logs 文件,分析一切可疑事件。如果在 errorlog 中出现 rm、login、/bin/perl、/bin/sh 等之类记录时,说明服务器可能已受到了非法用户的入侵。
- 设置 Web 服务器上系统文件的权限和属性,给可让访问的文档分配一个公用的组,比如可将 WWW 设置为只读权限。把所有的 HTML 文件归属 WWW 组,由 Web 管理员管理 WWW 组,对于 Web 的配置文件只有 Web 管理员才有写的权限。

6.3.3 IE 浏览器安全

1. 安全级别设定

如果想屏蔽 Cookie 与 ActiveX 控件功能,可以很容易地通过 IE 的安全级别设定功能加以实现。

IE 的安全机制共分为高、中、中低、低 4 个级别,分别对应着不同的网络功能。高级是最安全的浏览方式,但功能最少,而且由于禁用 Cookies 可能造成某些需要进行验证的站点不能登录;中级是比较安全的浏览方式,能在下载潜在的不安全内容之前给出提

示，同时屏蔽了 ActiveX 控件下载功能，适用于大多数站点；中低的浏览方式接近于中级，但在下载潜在的不安全内容之前不能给出提示，同时，大多数内容运行时都没有提示，适用于内部网络；低级别的安全机制不能屏蔽任何活动内容，大多数内容自动下载并运行，因此，它只能提供最小的安全防护措施。

操作步骤，单击 IE 浏览器"工具"|"Internet 选项"|"安全"，在安全级别设置窗口下，简单拖动滑块就能完成安全级别的设定。

2. 禁用自动完成功能

IE 的自动完成功能非常实用，可以让用户实现快速登录，快速填写的目的，但它的缺陷也同样明显。许多站点，在进行登录时会自动搜索与读取用户的历史操作以便获取用户信息，包括在地址栏中输入的历史地址，以及一些填过的表单信息；同时，对于经常在网吧上网，又不想让其他人知道自己历史操作的朋友，最好禁用 IE 的自动完成功能，因为后来者只需单击"历史"按钮就能让你的所有隐私无所遁形。

操作步骤，单击"工具"|"Internet 选项"|"内容"|"自动完成"，在对话框中清除相应栏目前面的选定符号就行了。

3. 清除历史记录

"历史"记录也是非常有用的一项功能，但对于公共用户，极容易造成个人隐私的泄露，因此，建议在离开计算机前清除历史纪录。

操作步骤，单击"工具"|"常规"|"清除历史记录"。

如果要清除单个网址记录，可以直接单击"历史"按钮，找到要删除的网址，单击鼠标右键，在弹出的下拉式菜单中选择"删除"命令。

4. 彻底清除 Cookies

IE 的"历史"记录并不是唯一记录上网操作过程的地方，许多站点在用户访问时会在用户计算机里放置一些小文件用以跟踪用户姓名、密码和访问时间等信息，而这些小文件就是 Cookies。可以通过安全机制的设定禁止 Cookies 功能，注意，在这种情况下是不能访问需要 Cookies 验证的网站。

彻底清除 Cookies 的步骤，在 IE 的"Internet 选项"中单击"删除 Cookies"按钮即可。

5. 启用分级审查功能

操作步骤，单击 IE 浏览器的"工具"|"Internet 选项"|"内容"|"分级审查"功能，并单击"启用"按钮，将会看到如图 6-3 所示的对话框，可以看到分级审查功能，共有 4 个审查标准，只需拖动滑动条进行设置。分级审查设定完成后会自动弹出一个"创建监督人密码"的对话框，如图 6-4 所示。这时，输入监督人密码后单击"确定"按钮。该密码是保护"分级审查"级别的设置。当用户再次要进入"内容审查程序"（如图 6-3 所示）进行分级审查设置时，必须提供正确的密码。

分级审查功能用以限制对具有暴力、色情及反动内容的网页、图片或文字进行浏览。



图 6-3　内容审查

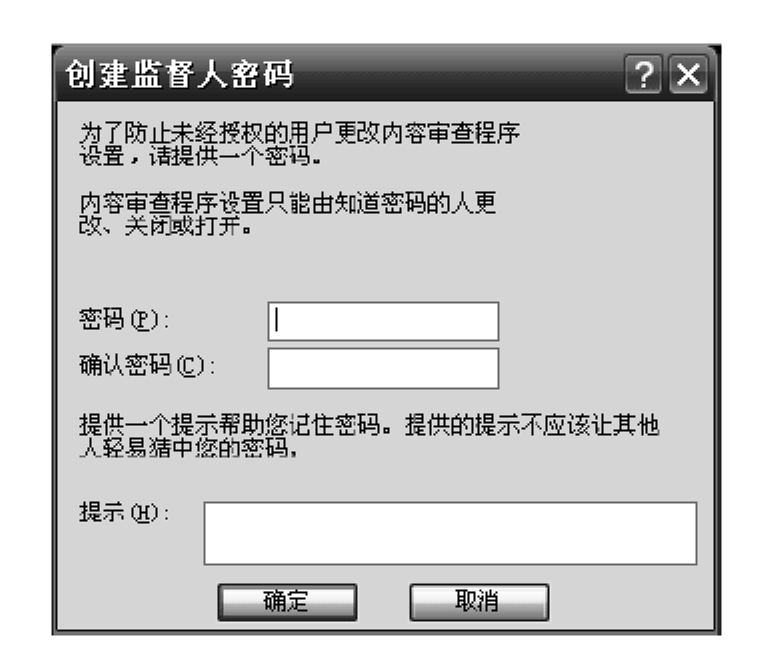


图 6-4　设置密码

6.4　电子邮件安全

6.4.1　电子邮件安全性分析

由于电子邮件的发送是要通过不同的路由器进行转发，直至到达电子邮件最终接收主机，攻击者可以在电子邮件数据包经过路由器的时候把它们截取下来，而且发件人对邮件是否被截获是毫不知情的。

使用电子邮件就像在邮局发送一封没有封口的信一样的不安全。从技术上看，没有任何方法能够阻止攻击者截取电子邮件数据包。唯一的办法就是让攻击者截获了数据包但无法阅读它，就是对电子邮件加密。当对电子邮件加密后，只要加密算法和密钥足够强大，那么即使攻击者截获了邮件数据也不能看到或修改邮件的内容。

电子邮件的收发方式有两种，一种是通过 Web 页方式收发信件，即用浏览器登录到主页来进行收发；另一种是使用邮件客户端，如 Outlook 和 Foxmail，使用这种方法的前提是邮件服务器必须支持 POP 协议。目前多数的免费信箱都支持这两种方式。

当用 Web 页方式收发信件时会存在以下问题。

1. 缓存漏洞

对于多数的浏览器来说，为了提高浏览速度，系统会自动将最近浏览过的网页保存到硬盘的某个临时文件夹里，这个文件夹称为缓存(cache)。当用户打开的网页关闭的时候，这些文件仍然可以轻易被读取。既然用户通过 Web 页方式读信，那么，这一封信实质上就是一个普通的网页，它同样会被保存在缓存里面。如果有人接触用户的硬盘文件，就没有任何秘密可言了。

2. 历史记录漏洞

这个漏洞的原理也很简单。事实上，每个信箱都能将用户名和密码通过特定的算法体现在 URL 上，浏览器的历史记录里恰恰会保存这一 URL 地址，如果有些信箱没有设置超时校验的话，任何人都可以通过查看本机的历史记录而进入信箱。

3. 攻击性代码漏洞

恶意的发件人可以将一段 Java Script 代码包含在给用户的邮件中，当用户浏览这个邮件时，系统会自动弹出一个对话框，提请用户重新输入用户名和密码登录，而事实上，用户输入的密码已经在幕后悄悄地发送到攻击者的手中。还有一种攻击手段就是，当打开邮件时，一段隐藏的程序代码已经设置好了自动转发功能，以后用户的任何一个邮件，都会自动复制一个副本寄到对它感兴趣的人手里。还有的代码可以开无数个窗口，使系统资源耗尽而最终死机。

总的来说，使用邮件客户端是比较安全的，但仍有几点应该注意。

- 尽量不要保存密码，因为密码框中的“*”号，在一些工具的帮助下就会原形毕露。
- 不要盲目信任有些密码，比如 Foxmail 的多账户。一个简单的调包就可以读到任何用户的信件而无需密码。
- 公用机器最好不要使用 POP 收发，即使一定要用，退出时也要将账号，以及属于用户的各个邮件文件夹一并删除。

6.4.2 匿名转发技术

所谓匿名转发，就是在隐藏发件人邮件地址的情况下将邮件转发。匿名邮件的转发技术有 3 种。

1. 初级方法

使用普通的邮件程序(如 Foxmail、IE 等)或一般 Web 信箱，只需在发件一栏填上一个假地址或错误的地址就行，或者让发件人一栏空着。但是此时发送的邮件不能做到真正匿名，因为收件人可以从邮件头上看出发件人上网时的 IP 地址、信件发送过程中所使用过的邮件服务器和信件发送时间。如果从邮件上看不到以上信息，只要稍微深究一下，比如在 Foxmail 中用鼠标右击该信件，再选中菜单中的“原始信息”，就能够让发件人“水落石出”了，因而这算不上真正的匿名邮件，也只能算是个骗骗菜鸟的初级方法。

2. 中级方法

如果有时间经常上网，又不怕浪费金钱，可以登录到提供免费发送匿名电子邮件服务的 Web 页面发送匿名电子邮件。有下列一些匿名邮件地址。

匿名邮件：http://voo.silversand.net/etc/n_mail.htm

浪潮金基匿名邮件发送：http://kahn.xj.cninfo.net/xinhai/service/fcd55.htm

Anonymizer 匿名邮件发送：http://personal.sd.cninfo.net/jgq/free/qita.html

发送方法非常简单，只要将对方信箱、主题、正文等分别填入相应的框中，再按“匿名发送”即可。

如果想节约时间和金钱，可以利用有些Internet服务机构提供的免费匿名邮件转发服务来发送，比如remailer@replay.com、mixmaster@remail.obscura.com.cn等。其方法是使用普通邮件程序比如IE或Foxmail等，在收件人一栏填入匿名邮件服务器的地址（不能填入真正收件人的地址），主题书写无限制，邮件正文格式是，第1行为空，第2行书写“::”，第3行书写“Anono:”后接着书写真正收件人的地址，第4行为空，第5行以后书写要发送邮件的内容。如果邮件程序中使用了签名功能或者使用的模板中有发件人的信息，记住一定要取消，否则会欲盖弥彰。

3. 高级方法

上述两种方法均无法发送邮件附件，在这里，介绍一款名叫Ghost Mail的匿名邮件软件，它的大小只有254K，可以到http://software.silversand.net83/internet/email/Ghostmail32.zip网站去下载。下载下来的Ghost Mail是一个ZIP格式的压缩文件，可以利用Winzip之类的压缩软件来把该文件解压缩到一个临时目录，然后直接用鼠标单击gm33.exe运行程序，就可以打开GhostMail的界面。该界面共有5个标签。

- From。填写发信人信息。
- To。填写收件人的E-mail地址和姓名信息。
- Type。选择是用该程序来发送匿名邮件还是张贴匿名新闻组。程序默认的设置是用来发送电子邮件用的；并且在该标签下用户还可以设置发送的内容是文本格式的还是HTML格式。
- Servers。设置通过哪一个匿名邮件服务器来发送邮件，可以采用这里的默认服务器mail.net.com，如果要填写另外的匿名邮件服务器的地址，必须要保证地址的正确性。
- Attach。加入邮件的附件。

6.4.3 E-mail炸弹

电子邮件炸弹（E-mail Bomb），是一种让人厌烦的攻击，也是黑客常用的攻击手段。传统的邮件炸弹大多是向邮箱内扔大量的垃圾邮件，从而充满邮箱，大量地占用系统的可用空间和资源，使机器无法正常工作。

E-mail炸弹常用的解救方法如下：

1. 向ISP求助

向ISP服务商求助，技术支持是ISP的服务之一，他们会帮用户清除电子邮件炸弹。

2. 用软件清除

利用邮件工具软件清除E-mail炸弹，这些软件可以登录邮件服务器，选择要删除哪些E-mail，保留哪些E-mail。

3. 利用 Outlook 阻止发件人功能

- 选中要删除的垃圾邮件。
- 单击“邮件”选项卡。
- 在邮件选项卡下有一个“阻止发件人”选项，拒收该邮件。

4. 用邮件程序的 E-mail-notify 功能过滤信件

使用邮件程序 E-mail-notify 功能可过滤和删除信件，E-mail-notify 不会把信件直接从主机上下载下来，只会把所有信件的头部信息(headers)送过来，它包含了信件的发送者、信件的主题等信息，用 View 功能检查头部信息，看到有来历可疑的信件，可从主机 Server 端直接删除掉。

5. 利用 IE 浏览器的 Internet 选项功能拒收信件

在 IE 浏览器中，选择“工具/Internet 选项/安全/受限站点”功能，将令人讨厌的发件者打入“黑名单”。凡打入了黑名单的邮件系统会拒收其发来的所有信息(包括电子邮件)。

6.5 FTP 与 Telnet 安全

6.5.1 FTP 存在的安全漏洞

1. 密码保护(protecting password)

存在的漏洞如下：

- 在 FTP 标准 PR85 中，FTP 服务器允许无限次输入密码。
- pass 命令以明文传送密码。

对此漏洞能够有两种强力攻击方式。

- 在同一连接上直接强力攻击，即不断进行密码尝试攻击。
- 与服务器建立多个、并行的连接进行强力攻击。

防范措施：服务器应限制尝试输入口令的次数，在几次(如 3 次)失败后服务器应关闭和用户的控制连接。在关闭之前，服务器有发送返回信息码 421(服务器不可用，关闭控制连接)。另外，服务器在响应无效的 pass 命令之前应暂停几秒钟来消除强力攻击的有效性。

2. 访问控制(access control)

存在漏洞：从安全角度出发，对一些 FTP 服务器来说，基于网络地址的访问控制是非常重要的。另外，客户端也需要知道所进行的连接是否与它所期望的服务器已建立。

防范措施：在建立连接前，双方需要同时认证远端主机的控制连接、数据连接的网络地址是否可信。

3. 端口盗用(port stealing)

存在漏洞：当使用与操作系统相关的方法分配端口号时，通常都是按增序分配。

攻击：攻击者可以通过端口分配规律及当前端口分配情况，只要攻击者知道了一个端口的分配情况，就可确定下一个要分配的端口，然后对端口做手脚。

防范措施：由操作系统随机分配端口号，让攻击者无法预测其他端口分配情况。

4. 保护用户名(user names)

存在漏洞：当 user 命令中的用户名被拒绝时，在 FTP 标准 PR85 中定义了相应的返回码 530。而当用户名有效时，FTP 将使用返回码 331。

攻击：攻击者可以通过 user 操作的返回码确定一个用户名是否有效。

防范措施：不论用户名是否有效 FTP 都应是相同的返回码，这样可以避免泄露有效的用户名。

5. 私密性(privacy)

在 FTP 标准 PR85 中，所有在网络上被传送的数据和控制信息都未被加密。为了保障 FTP 传输数据的私密性，应尽可能使用强大的加密系统。

6.5.2 FTP 安全技术

1. 匿名登录

用过 FTP 的人都知道，FTP 提供一种匿名服务(anonymous service)功能。登录名用 anonymous，而口令通常可用用户的电子邮件地址代替。正是这种服务方式方便了用户，但也不可避免地带来了安全问题，如客户登录后，往往能够获得一个可写目录，这样客户就可以通过 put 上传一个甚至是多个 txt 文件，来达到其攻击该 FTP 服务器或其他 FTP 服务器的目的。虽然许多 FTP 服务器都限制匿名用户的权限，比如执行权，但是许多 FTP 服务器与 Web 服务器同装在一台机器上，那么匿名用户完全可以利用该可写目录运行命令调用 Web 服务器执行。

2. FTP 代理服务器

通过 FTP 代理服务器连接到匿名 FTP 服务器，而不是直接连接到 FTP 服务器上。这样做的主要目的基于两个方面，第一，无法直接连接，比如存在防火墙；第二，出于不被匿名服务器知晓其 IP 地址的目的，或者登录者就是网络攻击者，或者由于匿名服务器根据 IP 地址来限制客户登录。

因此，对于防火墙内的客户来说，它必须先运行 FTP 命令并通过作为主机的防火墙

连接,连接完成后,必须说明用户名和连接地点,在认证该地点确实允许之后,代理才与远程系统上的 FTP 服务器建立连接,使用用户提供的用户名开始登录。然后,远程服务器提示用户输入口令,如果口令正确,则连接被允许。对于非防火墙内用户,它可以通过任意代理服务器来连接其目的服务器,并达到隐藏其地址的目的。对于目标服务器而言,其知道的仅仅是代理服务器的地址。

这样,通过 FTP 代理服务器对 FTP 服务器进行攻击,往往使得查找网络攻击源变得很困难,而且如果 FTP 服务器和 FTP 代理服务器间存在一定的信任关系,攻击就变得更容易了。

3. 跳板(bounce)攻击问题

FTP 的代理服务特性是允许第三方文件传输。一个用户可以从一个 FTP 向另一个远程 FTP 请求代理传输。实际上这种特性已在 RFC959 中被说明,当与引用命令相连时,例如 PORT 及 PASV 语句,允许一个用户避免 IP 访问控制及可跟踪性。

假设一个网络攻击者的 IP 地址是 221.210.0.10,他想从另一个目标服务器获得资源,但目标服务器对一些特定的 IP 地址范围进行了限制。假定网络攻击者的 IP 地址 221.210.0.10 恰好在这一限制范围内,因此目标服务器上的一些或所有的资源都不能访问,所以必须使用另一台机器(中继服务器)去访问目标服务器。其简单的过程就是,用户登录上这台中继网服务器后,向中继用服务器目录写一个文件,该文件包含有连接到目标机器并获取所需信息的命令。当该中介服务器连接目标服务器时,使用了它自己的地址而不是攻击者的地址。因此,目标服务器信任该连接请求并返回要求的文件。这样就构成了一个跳板攻击。

6.5.3 Telnet 安全性分析

Telnet 是一个非常有用的工具,并且一般主机都开启了 Telnet 服务。因此可以使用 Telnet 登录上一个开启了 Telnet 服务的主机来执行一些命令,便于进行远程工作或维护。

但 Telnet 本身存在很多的安全问题,描述如下:

- 传输明文。Telnet 登录时没有口令保护,远程用户的登录传送的用户名和密码都是明文,网络攻击者使用任何一种简单的嗅探器都可以截获。
- 没有强力认证机制,验证的只是连接者的用户名和密码。
- 没有完整性检查。传送的数据没有办法知道是否完整,不能判断数据是否被篡改过。
- 传送的数据都没有加密。中途的截获可以马上看到数据的内容。

解决办法:不要使用传统的明文软件 Telnet,而要使用 SSLTelnet 或 SSH 这样的对数据加密传输的软件。

6.6 IPv4与IPv6安全

6.6.1 IPv4安全性分析

目前广泛使用的TCP/IP协议是安全机制不完善的IPv4版本。该版本的TCP/IP协议体系中存在许多安全缺陷，列举如下：

- TCP/IP本身不提供加密传输功能，用户口令和数据是以明文形式传输的，很容易在传输过程中被截获或修改。
- TCP/IP本身不支持信息流填充机制，容易受到信息流分析的攻击。
- TCP/IP本身不提供对等实体鉴别功能，恶意的第三者实体可以轻易冒充合法用户与连接的一方通信，并能骗取对方的信任。
- TCP/IP协议体系本身存在缺陷，容易遭受到攻击，例如，服务端口的半开连接问题会造成拒绝服务现象发生。
- 由TCP/IP支持的Internet中的各个子网是平等的，难以实现分级安全的网络结构(如树状结构)，无法实现有效的安全管理。
- 许多厂商提供的TCP/IP应用层协议实用软件中存在严重的安全漏洞，常常被黑客用作网络攻击的工具。

综上所述，TCP/IP协议体系中确实存在严重的安全缺陷，但它的协议却又被广泛使用，因此必须重视研究与解决TCP/IP体系的安全问题。

6.6.2 IPv6安全性分析

IPv4是整个Internet网络的基本通信协议，从1970年底问世以来不断地更新。随着通信技术和计算机技术的发展，Internet网络性能不断提高，应用越来越广泛。因此，尽管IPv4的设计是健全的，但它必然被取代，即用IPv6取代IPv4。

下一代IP协议是IPv6。IPv6除了对IP地址作了较大的改动以外，也完全改变了IPv4的数据包格式。如图6-5所示，IPv6数据包有一个固定大小的基本首部(base header)，其后可以允许有零个或多个扩展首部(extension header)，再其后才是数据信息。

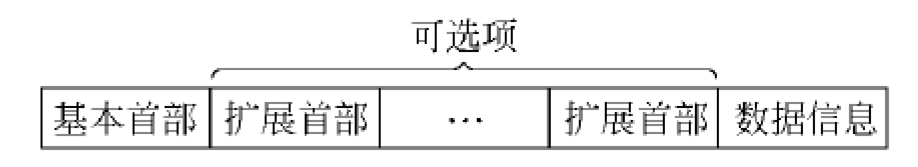


图6-5 IPv6数据包的一般格式

IPv6在安全性能方面具有较大提高，它主要是利用了IPSec(Internet Protocol Security，因特网安全协议)，IPSec在网络协议栈的IP(Internet Protocol)层提供加密和认证服务技术。IPsec包含三个安全措施，认证头AH(Authentication Head)，提供封包层的认证服务和封装安全净荷ESP(Encapsulating Security payload)，提供加密以及认证服务、

Internet 密钥交换协议 IKE(Inter Key Exchange),用以对通信双方提供身份认证和密钥交换方法。在 IPv6 中,AH 和 ESP 都作为一个扩展首部。IPv6 和 IPv4 安全性的最大不同就是 IPSec 是作为一种附加的安全措施作用于 IPv4 的,而 IPv6 的所有产品的安全措施则是以 IPSec 为主。

1. 加密和认证

AH 提供了认证机制,通过这个认证过程可保证数据包接收者得到的源地址是可靠的,且所接收的数据包在传输过程中没有被篡改或更换。ESP 保证只有合法的接收者才能读取数据包的内容。这两者都是建立在安全关联(security association)的概念基础上。

1) 安全关联

认证和加密要求发送者和接收者就密钥、认证或加密算法以及一系列附属特性(如密钥生命周期、算法使用细节等)达成一致的协定。这套协定机制组成了发送者和接收者之间的一种"安全关联"。接收者在收到数据包后,只有在能将其与一种安全关联的内容相关联起来时,才能对其进行验证和解密。所有的 IPv6 验证和加密数据包都带有安全参数索引(Security Parameter Index,SPI)。

当数据包通过单播地址只发送给一个接收者时,SPI 就由该接收者来选定,例如它可以是接收者所维持的安全上下文表的索引。事实上,一台主机每次接收时所使用的 SPI 都是"安全关联"中的一个参数。每台工作站都必须记住其对端使用的 SPI,以便识别安全上下文。

当数据包通过多播地址发送给一组接收者时,SPI 对组中的所有成员是同等对待的。每个成员都能将组地址和 SPI 结合起来,并与密钥、算法和其他参数产生关联。通常,对 SPI 的协商操作是在密钥交换过程中进行的。

2) 认证头

认证头 AH 是 IPv6 所定义的扩展报头中的一种,由有效负载类型 51 来标识。例如,一个被认证的 TCP 数据包会包括有一个 IPv6 报头、一个认证报头和 TCP 数据包本身。除此之外,还有其他几种变体,例如在 AH 前插有路由选择报头,或者在 AH 和有效负载之间插入端到端选项等,如图 6-6 所示。

IPv6 报头	AH	TCP 报文段

IPv6 报头	路由报头	AH	TCP 报文段

IPv6 报头	AH	端到端选项	TCP 报文段

图 6-6 认证过的 TCP 数据包举例

认证头的出现不会改变 TCP 的行为,事实上也不会改变任何端到端协议,如 UDP 和 ICMP。它所提供的就是对数据原始性的明确担保。尽管在实际中端到端协议也可以用来拒绝任何没有被认证的数据包。

认证头的语法很简单。开始部分是一个 96 位的报头,包括下一个报头的编号、认证有效负载的长度、必须设置为 0 的 16 个保留位、安全关联用的 32 位 SPI 以及一个 32 位

的序列号。紧随这组固定长度参数之后的就是认证数据，其编码为一组可变长度的 32 位字，例如，如果认证数据长为 96 位，则长度值就设置为 4。认证报头的格式如图 6-7 所示。

0 下一个报头	10 有效净荷长度	21 保留 31
SPI		
序列号字段		
认证数据（长度是可变的）		

图 6-7 认证报头格式

序列号字段是在安全规范的 1997 年修订版中加入的。发送者在安全关联的数据中加入编号，接收者使用此编号来识别并废弃过时的数据包。这样就可以防止“重放”的攻击，攻击者在获取到一份有效的数据包备份后，进行处理再重新放到网上。不过，实施这种保护措施要慎重小心，因为因特网并不保证对数据包进行有序发送。接收者应该将每一个安全关联都与最高的序列号 N 关联，即在一个经过正确认证的数据包里已经收到的所有序列号进行关联。

在这里，应该注意，若允许循环，则序列号并不能完全保证免受重放的攻击。如果一次安全关联过程中所传输的数据包超过 2^{32} 个时，序列号就会出现循环。要想取得更好的安全性，在出现循环之前就应重新协商新的密钥。

认证数据来源于加密校验和的计算。这种计算所涉及的内容包括有效负载数据、IPv6 报头和扩展报头中的某些字段，以及关联成员所约定的秘密值。认证数据的精确长度取决于计算校验和所选定的算法。接收者将根据数据包的内容和 SPI 指引处的秘密值计算出一个预期值，再把它与数据包中所收到的认证数据的计算结果相比较。如果二者相等，就可以证明数据包是由知道此秘密值的主机发送的，并在传播中未被更改。

认证头的使用将能有效地防止目前因特网上屡见不鲜的地址欺骗攻击，同时它还能保护用户连接不被盗用。

3）计算认证数据

认证头用户保护数据报的完整性以及证实其内容在传输过程中未被修改。然而，存在的问题是有些字段在传输过程中必须要做修改。在 IPv6 报头中，每经过一跳，跳数值就要自动减 1。如果用到了路由选择头，IPv6 的目的地址和下一个地址就会在源路由的每次中继时进行交换，同时下一个地址进行递增。某些端到端选项可能也会在传输中更新，这点由选项类型中的“在路由中改变”值位来表示。

为了解决这个问题，在计算认证数据之前，发送者就必须准备一个该报文的特殊版本，与传输中的转换无关。在 IPv6 报头中，第一个 32 位不参与计算；在 IPv6 报头中，跳数设为 0；如果用到了路由选择报头，那么 IPv6 的目的站点就设为最终的目的站点，路由选择报头的内容设为它即将到达的站点值，并对地址索引做相应设置。

在这里，校验和是使用一种特殊的加密算法计算得到的。常规的校验和算法，比如在串行链路和以太网中所使用的传统 IP 的 16 位校验和或者 16 或 32 位多项式校验和算法等，在这里都不能使用。因为这些算法只能用来防止由噪音引起的随机错误对报文造

成的干扰，而并不能防止入侵者的人为进攻。

在 IPSec 中所建议的算法是 keyed MD5，即带密钥的 MD5 算法。具体做法是，将报文与密钥结合后，再对其结果计算散列值。密钥放在报文的起始或末尾，这样能防止某些类型的攻击。

将校验和缩短到 96 位将保持 AH 的大小为 M 个字节，即 64 位的倍数，而不会削弱认证能力。

实际应用中，认证算法是在安全关联的建立过程中协商的。MD5 算法只有在确保所有实现方法中至少有一种共同算法时才能被指定为默认算法。

4）封装安全净荷

认证头并不对数据进行加密，当要求保密时就应该使用封装安全净荷 ESP。ESP 报头在 IPv6 报头链中总是在最后的位置，并处于加密部分的最外层，如图 6-8 所示。

ESP 的序列号和 AH 的序列号极为相似，它用来保护接收者免受重放攻击。在加密数据之后的认证检验和保护接收者免受一种将加密数据切碎或截短的攻击。用来结合校验和的算法是安全关联的一个参数。在任何情况下，校验和都是用来保护序列号和加密数据的。ESP 的格式如图 6-9 所示。

IPv6报头
扩展报头
ESP报头
加密数据
认证数据

图 6-8　使用 ESP 报头的加密数据包

32位 SPI
32位序列号
加密数据和参数
认证数据

图 6-9　ESP 的通用格式

实际上，ESP 具体的格式与所使用的加密算法有关。规范中所建议的默认算法是用 DES-CBC（Data Encryption Standard-Cipher Block Chaining，数据加密标准-密码分组链接模式），与 MD5 在认证中的情况相同，DES-CBC 是默认算法，在安全关联建立后也可以选用其他算法。

当同时要求采用认证和保密时，可以同时使用 AH 和 ESP，并且建议总是将 ESP 置于 AH 中。这样接收者既不需要在解密前检查报文的真实性，也不需要在做可靠性检查的同时进行解密。

2. 密钥的分发

安全关联的建立依赖于只有参与关联的成员才知道密钥的存在，而安全性的有效扩散要依赖于有效的密钥分发方法。密钥管理和安全协议的链接实际上就是安全关联的安全参数索引。因特网机构正在统一密钥分发方案，如 Photuris、SKIP 和 OAKLEY 等。

因特网安全协会和密钥管理协议（ISAKMP）为密钥交换协议的实现提供了一个非常通用的框架。所有的 ISAKMP 报文都具有相同的报头，紧随其后的是 ISAKMP 有效负载清单。这些报文通常使用第 500 端口通过 UDP 交换。单一的事务可以同时为几个协议建立密钥。例如，用于两个独立的加密和认证协议，属于同一个协议的有效负载放

在一个定义协议标志的(封装的)有效负载后面。

6.6.3 IPv6安全机制

IPv6 安全机制有很多潜在的应用,最引人注目的如在防火墙之间的应用、移动主机和基站之间的应用以及安全主机之间的应用。认证过程可以非常有效地保护建网过程,比如邻机发现或路由信息交换等。

1. 管道和防火墙

目前因特网安全机制的实现在很大程度上都依赖于防火墙。IPv6 的 AH 和 ESP 报头可用来在两个远距离防火墙之间建立安全通道,例如,在同一公司的两台终端之间的距离安全通道,如图 6-10 所示。



图 6-10 两个防火墙之间的安全通道

两个终端之间的数据包交换将封装到 IPv6 的数据包中,从一个防火墙通过因特网传到另一个防火墙。如果仅要求认证则使用 AH 即可,如果还需要对数据加密,则还将使用到 ESP。如果使用认证,终端 1 与终端 2 之间所交换的典型数据包将在防火墙 F1 与防火墙 F2 先后进行两次转换,即由 F1 封装,由 F2 解封。

如果使用认证,黑客就无法插入伪造数据包;如果使用加密,黑客就无法看穿管道。

2. 移动主机

移动主机备受安全组织的关注。因为移动主机可以连接到任何一种远程网络,而不受组织管理者的控制。

一个防止特殊攻击的方法是在移动计算机和基地防火墙之间建立安全通道,如图 6-11所示。如果防火墙对于移动主机来说作为基地网,对于邻机发现来说作为代理机,则这个解决方案可以和 E 等级移动程序相结合。这样移动主机则有两个地址,一个在远程网;另一个在基地网。和移动主机基地地址捆绑的数据包将通过使用安全封装的防火墙中继。



图 6-11 移动单元和防火墙间的安全通道

3. 邻机发现

ICMP 最重要的功能之一是邻机发现。利用邻机发现功能,系统能找出该链路上的其他主机和路由器。系统通过对同一链路上主机的学习,能够传送链路上主机期待的数据报。主机为了向不在同一链路上的系统传送数据报,至少要学习一个路由器。当主机选择了低效的路由器时,还可以利用邻机的学习,使路由器向主机指示最适用的路由器。

某些建网过程有特殊的安全需求。邻机发现是一个很好的例子。可以控制对网络的访问,以便做到只允许有明确授权的访问者才能将其便携机接入用户的网络。还可以控制对某些报文的授权,以便工作站及时中止向错误的地址传送数据。

路由公告是发给多播组中的所有结点的。通过定义 SPI,人们很容易为该组配置一个安全关联。需要注意的是,像 MD5 这样的算法仅能保护这个组不受外来者侵犯。由于密钥是本组工作站所共知的,因此,每个工作站都可以以一个路由器的方式出现。利用路由公告信息,任何黑客都可以将一台计算机连接到本地网络上。

邻机公告是发送给请求者的单播地址的。只有在邻机和请求者之间建立了安全关联的情况下邻机公告才是安全的。如果双方还没有交换任何一个数据包,那么它们怎么能协商密钥呢? 对此问题有两种答案,网管人员可让工作站在下一阶段再协商一个安全关联;也可以对路由器编程,使其不广播本地地址前缀,迫使主机总以路由器作为它们的第一个下一跳站点,并且在本地通信中依靠已认证的重定向报文。

4. 路由选择协议

如果路由选择协议不安全,那么整个网络将无法维持。因为入侵者可以伪装路由选择更新报文,并且可以中断通信或转移某些连接。使用 IP 安全机制对定义特定路由器之间的认证和加密函数来说是最佳的技术手段。

6.7 应用实例

6.7.1 IP地址与MAC地址的绑定技术

1. IP 地址与 MAC 地址的绑定

使用 IP 地址与 MAC 地址绑定技术能有效地防止 IP 地址被盗用,其操作方法是利用 Windows 提供的 arp 命令,命令格式为:

```
arp -s <IP地址> <MAC地址>
```

例如,使用 arp -s 192. 168. 1. 2 00-A0-43-E0-6A-84 的命令,能将静态 IP 地址192. 168. 1. 2与网卡地址为 00-A0-43-E0-6A-84 的计算机绑定在一起,别人就不能使用这个 IP 地址了。

上面的方法虽然可以在一定程度上解决非法用户网络接入的问题和 IP 地址冲突的

问题,但非法用户还是可以通过修改注册表,下载专用修改 MAC 小工具等方法,轻松更改本机的 MAC 地址,甚至将本机的 MAC 地址和其他 IP 地址进行绑定,这样,非法用户就可以使用网络了。

2. 交换机的 MAC 地址与端口绑定

可以将 MAC 地址与交换机的以太端口绑定,若非法用户擅自改动本机的 MAC 地址而试图访问网络,因其 MAC 地址被交换机认定为非法而无法达到目的。

在这里以 Cisco 交换机为例。

登录进入交换机,输入管理口令进入配置模式。

```
(config)# mac_address_table permanent [MAC 地址] [以太网端口号]
```

逐一地将每个端口与相应的计算机 MAC 地址进行绑定,保存退出后就彻底阻止了用户的非法修改。

6.7.2 上网助手的使用技术

人们上网使用最多的功能就是使用 IE 浏览器浏览各种网站及其网页,“YAHOO 上网助手”就是针对 IE 浏览器进行管理的,其主界面如图 6-12 所示。



图 6-12 上网助手主屏幕

“YAHOO 上网助手”的功能很多,在这里介绍几个常用的功能。

1. 清理 IE 地址

如果用户不想让别人知道自己上网时浏览了哪些网站,可利用“上网助手”|“清理 IE 地址”功能将有关 IE 地址清除。

在如图 6-13 所示的“清理 IE 地址栏”窗口中,选定相应的 IE 地址并单击“立即清理”按钮,即自动将相关的 IE 地址在 IE“地址”栏中消除。



图 6-13　清理 IE 地址

2. 全面清理上网痕迹

清理 IE 地址功能只能清理 IE“地址”栏中的 IE 地址，而使用“全面清理”功能则可将所有上网痕迹全部清除。

全面清理操作窗口如图 6-14 所示。



图 6-14　全面清理上网痕迹

3. IE 修复专家

只要使用 IE 上网，用户的计算机就有可能受到攻击，其中 IE 浏览器本身也不例外。

当 IE 浏览器受到攻击后，会出现浏览器工作不正常的现象，严重时 IE 浏览器根本不能工作。

使用“IE 修复专家”功能，可以修复 IE 浏览器，特别是使用“强力修复”功能，可以使浏览器复原到最原始的状况。IE 修复专家如图 6-15 所示。



图 6-15　IE 修复专家

4. 广告拦截

只要连接到 Internet 网络上，各种各样的广告就会铺天盖地地向连接的计算机扑来，让用户困惑和心烦。如果不希望无关的广告“骚扰”，可使用“上网助手”的“广告拦截”功能屏蔽广告。

图 6-16 是广告拦截窗口。使用方法是：首先用“开启广告拦截”选项卡进行拦截广告类型设置，然后用“高级设置”选项卡进行拦截级别设置，并单击“确定”按钮。可用“拦截

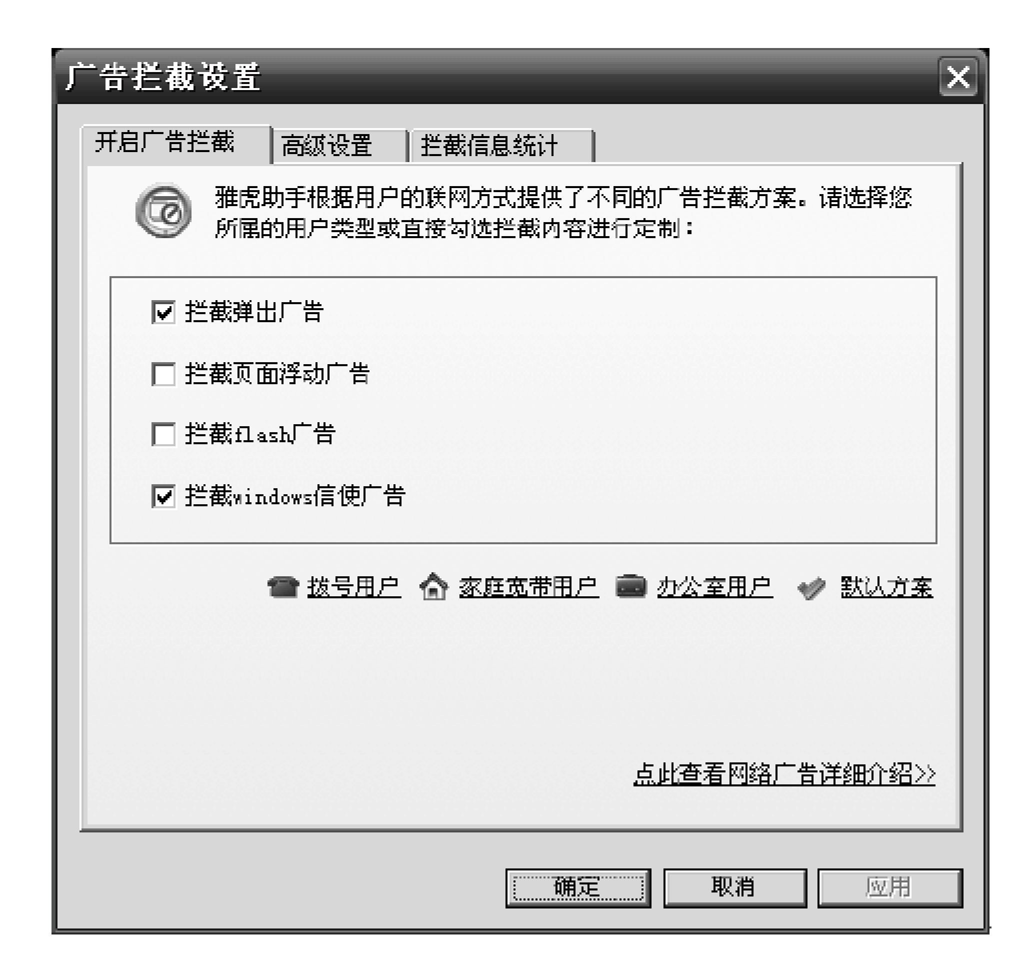


图 6-16　广告拦截

信息统计”选项卡查看广告拦截情况。

5. IE 插件管理

使用“IE 插件管理”功能可对网页中各种弹出式窗口进行管理，即可屏蔽用户不希望在 IE 浏览器中看到的弹出窗口。IE 插件管理如图 6-17 所示。



图 6-17 IE 插件管理

6.7.3 缓冲区溢出的防范技术

1. 缓冲区溢出及堆栈溢出

1）缓冲区溢出

究竟什么缓冲区溢出漏洞，溢出究竟是怎么发生的。先看下面一段简单的 C 程序代码：

```
# include< stdio.h>
void main()
  {
    char buf[8];
    gets(buf);
  }
```

程序运行的时候，如果输入 Hello，或者 Kitty，那么程序运行一切正常，但是如果输入 Today is a good day(这里有 17 个字符而要占 18 个字节，因为字符串的最后系统会自动添加一个结束符)，程序将会发生溢出。特别要注意的是，当输入的字符刚好是 8 个字符的字符串 Than You 时也会发生溢出，这是 C 语言的字符串系统自动会在后面加入一个结束符“\0”所致。很显然，buf 这个数组只申请了 8 个字节的内存空间，而输入的字符

却超过了这个数目，于是，多余的字符将会占领程序中不属于自己的内存。因为 C/C++ 语言并不检查边界，于是，程序将看似正常继续运行。如果被溢出部分占领的内存并不重要，或者是一块没有使用的内存，那么，程序将会运行直至结束。但是，如果溢出部分占领的正好是存放了程序重要数据的内存，那么一切后果将会不堪设想。

下面再举一个缓冲区溢出的例子。在这一例子中，假设变量 aa1、aa2 和 aa3 所分配的是一片连续的内存单元。

```
#include <stdio.h>
void main()
{char aa1[ ]={"012345678\0abcdefg\0"};
char aa2[10],aa3[8]={"Chinese\0"};
int i,j;
for (i=0;i<18;i++ )
 {aa2[i]=aa1[i];}
    printf("\n aa2=% s aa3=%s",aa2,aa3);
 }
```

在这一段 C 程序中，定义了 3 个缓冲区 aa1、aa2 和 aa3，并对 aa1 和 aa3 分别赋初值为“012345678\0abcdefg\0”和“Chinese\0”，而 aa2 未赋初值。这里的“\0”为字符串结束符。

程序运行时，通过 for (i=0;i<18;i++) {aa2[i]=aa1[i];}循环语句将缓冲区 aa1 的值赋给 aa2(共 19 个字符)，由于缓冲区 aa2 只定义了 10 个字节长度，所以只能存放 aa1 的前 10 个字符，即“012345678\0”，而 aa1 第 11 个以后的字符则放在了缓冲区 aa2 之后的存储单元 aa3 中。所以，当程序运行结束时，缓冲区 aa3 中的内容已不再是“Chinese\0”而是“abcdefg\0”。程序运行结果如下：

```
aa2=012345678    aa3=abcdefg
```

实际上，缓冲区溢出通常有两种：堆溢出和堆栈溢出。尽管两者实质都是一样的，但利用的方式不同，将在下面分别介绍。

通常在程序运行时，内存中包含下述内容。

- 程序参数和程序环境。
- 程序堆栈。通常在程序执行时增长，向下朝堆增长。
- 堆。也在程序执行时增长，相反，向上朝堆栈增长。
- BSS 段。包含未初始化的全局可用的数据(例如全局变量)。
- 数据段。包含初始化的全局可用的数据(通常是全局变量)。
- 文本段。包含只读程序代码。
- BSS、数据和文本段组成静态内存。在程序运行之前这些段的大小已经固定。程序运行时虽然可以更改个别变量，但不能将数据分配到这些段中。

下面以一个简单的例子来说明。

```
#include<stdio.h>
```

```
char buf[3]= "abc";
int i;
void main()
  {
    i=1;
    return;
  }
```

其中,i 属于 BBS 段,而 buf 属于数据段。两者都属于静态内存,因为他们在程序中虽然可以改变值,但是其分配的内存大小是固定的,若 buf 的数据大于 3 个字符,将会覆盖其后内存单元的数据。

与静态内存形成对比,堆和堆栈是动态的,可以在程序运行的时候改变大小。堆的程序接口因语言而异。在 C 语言中,堆是经由 malloc() 和其他相关函数来访问的,而 C++ 中的 new 运算符则是堆的程序接口。堆栈则比较特殊,主要是在调用函数时用来保存现场,以便函数返回之后能继续运行。

2) 堆溢出

堆溢出的思路很简单,覆盖重要的变量以达到自己的目的。而在实际操作的时候,这显得比较困难,尤其是源代码不可见的时候。第一,必须确定哪个变量是重要的变量;第二,必须找到一个内存地址比目标变量低的溢出点;第三,在特定目的下,还必须让在为了覆盖目标变量而在中途覆盖了其他变量之后,程序依然能运行下去。下面是一个堆溢出的例子。

```
#include "malloc.h"
#include "string.h"
#include "stdio.h"
void main()
{char * large_str = (char * )malloc(sizeof(char) * 1024);
char * important= (char * )malloc(sizeof(char) * 6);
char * str = (char * )malloc(sizeof(char) * 4);
strcpy(important,"abcdef");   //* 给 important 赋初值
//* 下面的两行代码是为了查看 str 和 important 的地址。
printf("%d\n",str);
printf("%d\n",important);
gets(large_str);              //* 输入一个字符串
strcpy(str,large_str);        //* 将输入的字符串复制到 str
printf("important :%s\n",important);
printf("str:%s\n",str);}
```

在这一程序中,所达到的目标是在没有给变量 important 赋值的情况下使其内容为 hacker。

str 和 important 的地址在不同的运行环境中是不同的,在这里,假定 str 和 important 的内存地址分别为 xxxx2146 和 xxxx2130。important 的地址比 str 大,这就为溢出创造

了可能。通过计算可知，两地址间间隔了16个字节。在程序运行时，输入字符串"1234567890abcdefhacker"。从程序执行过程中可看出，虽然只给变量large_str输入字符串"1234567890abcdefhacker"，并将其复制到str中，并没有对important重新赋值，但其结果是important的内容变成了hacker。

3）堆栈溢出

堆溢出的一个关键问题是很难找到所谓的重要变量，而堆栈溢出则不存在这个问题，因为它将覆盖一个非常重要的内容，函数的返回地址。在进行函数调用的时候，断点或者说返回地址将保存到堆栈里面，以便函数结束之后能继续从该处运行。而堆栈溢出的思路就是在函数里面找到一个溢出点，把堆栈里面的返回地址覆盖，替换成一个自己指定的地址。这里的目标是写出一个通过覆盖堆栈返回地址而让程序执行到另一个函数的堆栈溢出演示程序。

因为堆栈是往下增加的，因此，先进入堆栈的地址反而大，这为在函数中找到溢出点提供了可能。试想，如果堆栈是往上增加的，那么将永远无法在函数里面找到一个溢出点去覆盖返回地址。用一个简单的例子进行说明。

```
void test(int i)
{char buf[12];
printf("&i=%d\n",&i);
printf("&buf[0]=%d\n",buf);}
void main()
{test(1);}
```

test函数具有一个局部参数和一个静态分配的缓冲区。

在这里，假设输出结果为&i=6684072 &buf[0]=6684052。当调用一个函数的时候，首先是参数入栈，然后是返回地址。并且，这些数据都是倒着表示的，因为返回地址是4个字节，所以可以知道，返回地址应该是保存在6684068～6684071之间。因为数据是倒着表示的，所以实际上返回地址就是：

buf[19]*256*256*256+buf[18]*256*256+buf[17]*256+buf[16]。

所要求的目标还没有达到，下面继续。在上面程序的基础，修改成：

```
#include< stdio.h>
void main()
{void test(int i);
test(1);}
void test(int i)
{void come();
char buf[12];//用于发生溢出的数组
int addr[4];
int k=(int)&i-(int)buf;//计算参数到溢出数组之间的距离
int go=(int)&come;
//由于EIP地址是倒着表示的,所以首先把come()函数的地址分离成字节
addr[0]=(go<< 24)>>24;
```

```
addr[1]=(go<< 16)>>24;
addr[2]=(go<< 8)>>24;
addr[3]=go>>24;
//用 come()函数的地址覆盖 EIP
for(int j=0;j< 4;j++ )
{buf[k-j-1]=addr[3-j];}}
void come()
{printf("Success!");}
```

程序运行之后,字符串 Success! 成功地显示出来。注意,由于这个程序破坏了堆栈,在运行过程中会提示:Abnormal program termination。

2. 如何应对缓冲区溢出漏洞攻击

目前有 4 种方法保护缓冲区免受缓冲区溢出的攻击和影响。即编写正确的代码、非执行的缓冲区、数组边界检查及程序指针完整性检查。

1) 编写正确的代码

编写正确的代码是一件非常有意义但耗时的工作,特别是像编写 C 语言那种具有容易出错倾向的程序(如字符串的结束符),这种风格是由于采用了追求性能而忽视正确性的传统方法引起的。尽管花了很长的时间但依然有安全漏洞的程序存在。因此人们开发了一些工具和技术来帮助经验不足的程序员编写安全正确的程序。

最简单的方法就是用 grep 来搜索源代码中容易产生漏洞的库的调用,比如对 strcpy 和 sprintf 的调用,这两个函数都没有检查输入参数的长度。事实上,各个版本 C 的标准库均有这样的问题存在。为了寻找一些常见的诸如缓冲区溢出和操作系统漏洞,一些代码检查小组检查了很多的代码。然而依然有漏网之鱼存在。尽管采用了 strcpy 和 sprintf 这些替代函数来防止缓冲区溢出的发生,但是由于编写代码的问题,仍旧会有这种情况发生。比如 lprm 程序就是最好的例子,虽然它通过了代码的安全检查,但仍然有缓冲区溢出的问题存在。

为了解决这些问题,人们开发了一些高级的查错工具,如 faultinjection。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。还有一些静态分析工具用于侦测缓冲区溢出的存在。虽然这些工具可以帮助程序员开发更安全的程序,但是由于 C 语言的特点,这些工具不可能找出所有的缓冲区溢出漏洞。所以,侦错技术只能用来减少缓冲区溢出的可能,并不能完全地消除它的存在,除非程序员能保证他的程序万无一失。

2) 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行,从而使得攻击者不可能执行被植入被攻击程序输入缓冲区的代码,这种技术被称为非执行的缓冲区技术。事实上,很多旧版本的 UNIX 系统都是这样设计的,但是近来的 UNIX 和 MS Windows 系统为实现更好的性能和功能,往往在数据段中动态地放入可执行的代码。所以为了保持程序的兼容性不可能将所有数据段设计成不可执行。但是可以设定堆栈数据段不可执行,这样就可以最大限度地保证了程序的兼容性。Linux 和 Solaris 都发布了有关这方面的内核补丁。

3）数组边界检查

植入代码引起缓冲区溢出是一个方面，扰乱程序的执行流程是另一个方面。不像非执行缓冲区保护，数组边界检查完全能避免缓冲区溢出的产生和攻击。这样，只要数组不能被溢出，溢出攻击也就无从谈起。为了实现数组边界检查，所有的对数组的读写操作都应当被检查以确保对数组的操作在正确的范围内。最直接的方法是检查所有的数组操作，通常可以用一些优化的技术来减少检查的次数。目前有以下的几种检查方法。

（1）Compaq C 编译器。

Compaq 公司为 Alpha CPU 开发的 C 编译器支持有限度的边界检查。这些限制是，只有显示的数组引用才被检查，比如“a[3]”会被检查，而“*（a+3）”则不会。由于所有的 C 数组在传送的时候是指针传递的，所以传递给函数的数组不会被检查。带有危险性的库函数如 strcpy 不会在编译的时候进行边界检查。在 C 语言中利用指针进行数组操作和传递是非常频繁的，因此这种局限性是非常严重的。通常这种边界检查用来进行程序的查错，而且不能保证不发生缓冲区溢出的漏洞。

（2）Jones&Kelly（C 的数组边界检查）。

Richard Jones 和 Paul Kelly 开发了一个 gcc 的补丁，用来实现对 C 程序完全的数组边界检查。由于没有改变指针的含义，所以被编译的程序和其他的 gcc 模块具有很好的兼容性。更进一步的是，他们由此从没有指针的表达式中导出了一个“基”指针，然后通过检查这个基指针来侦测表达式的结果是否在容许的范围之内。当然，这样付出的性能上的代价是巨大的，对于一个频繁使用指针的程序，如向量乘法，会由于指针的频繁使用而使速度慢若干倍。

（3）Purify（存储器存取检查）。

Purify 是 C 程序调试时查看存储器使用的工具而不是专用的安全工具。Purify 使用“目标代码插入”技术来检查所有的存储器存取。通过用 Purify 连接工具连接，可执行代码在执行的时候带来性能的损失会使程序的运行速度下降若干倍。

（4）类型——安全语言。

所有的缓冲区溢出漏洞都源于 C 语言的类型安全。如果只有类型-安全的操作才可以被允许执行，这样就不可能出现对变量的强制操作。如果作为新手，可以推荐使用具有类型-安全的语言，如 Java 和 ML。

4）程序指针完整性检查

程序指针完整性检查和边界检查略有不同。与防止程序指针被改变不同，程序指针完整性检查在程序指针被引用之前进行检测。因此，即便一个攻击者成功地改变程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不会被使用。与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但是这种方法在性能上有很大的优势，而且兼容性也很好。

（1）堆栈保护。

堆栈保护是一种提供程序指针完整性检查的编译器技术，通过检查函数活动纪录中的返回地址来实现。堆栈保护是在每个函数中，加入了函数建立和销毁的代码。加入的

函数建立代码实际上在堆栈中函数返回地址后面加了一些附加的字节。而在函数返回时,首先检查这个附加的字节是否被改动过,如果发生过缓冲区溢出的攻击,那么这种攻击很容易在函数返回前被检测到。但是,如果攻击者预见到这些附加字节的存在,并且能在溢出过程中同样地制造他们,那么它就能成功地跳过堆栈保护的检测。

(2) 指针保护。

在堆栈保护设计的时候,冲击堆栈构成了缓冲区溢出攻击的常见形式。有人推测存在一种模板来构成这些攻击。因此,很多简单的漏洞被发现,很多攻击者开始用一般的方法实施缓冲区溢出攻击。指针保护是堆钱保护的推广。通过在所有的代码指针之后放置附加字节来检验指针在被调用之前的合法性,如果检验失败,会发出报警信号和退出程序的执行,就如同在堆栈保护中的行为一样。

习 题 6

1. 局域网络安全涉及哪些内容?
2. 局域网络在安全方面存在哪些缺陷?
3. 局域网络的安全措施包括哪几个方面?
4. 广域网安全策略是什么?
5. 无线局域网的安全技术主要有哪些?
6. OSI 安全模型是什么?
7. TCP/IP 安全模型是什么?
8. Web 服务器的安全预防措施是什么?
9. 如何设置 IE 浏览器的安全级别?
10. 什么是电子邮件炸弹?
11. IPv4 安全性包括哪些内容?
12. IPv6 的安全性包括哪些内容?
13. 应对缓冲区溢出漏洞攻击有哪些措施?

第 7 章 chapter 7

网络操作系统安全

网络操作系统很多，有 Novell 公司的 Netware，Microsoft 公司的 Windows NT Server、Windows 2000/2003 Server，还有 UNIX、Linux 等。在这一章中，介绍两款常用的网络操作系统，Windows 2000/2003 Server 和 UNIX 的安全技术。

7.1 Windows 2000/2003 Server 安全

7.1.1 Windows 2000 Server 安全

Microsoft 公司的 Windows 2000 Server 操作系统因其界面友好直观、操作方便、功能强大而受到广大用户的青睐，很多的应用系统都运行在 Windows 2000 Server 操作系统上。如何才能搭建一个安全的操作系统是安全管理人员所关心的问题。

1. Windows 2000 Server 操作系统安全分析

1）系统安装隐患

在一台服务器上安装 Windows 2000 Server 操作系统，主要存在以下安全隐患：

- 将服务器接入网络进行系统安装。Windows 2000 Server 操作系统在安装时存在一个安全漏洞，当输入 Administrator 密码后，系统就自动建立了 ADMIN $ 的共享，但是并没有用刚刚输入的密码来保护它，这种情况一直持续到再次启动计算机，在此期间，任何人都可以通过 ADMIN $ 进入这台机器；同时，只要安装一结束，各种服务就会自动运行，而这时的服务器是满身漏洞，计算机病毒非常容易侵入。因此，若将服务器接入网络后再进行操作系统的安装是很不安全的。
- 操作系统与应用系统共用一个磁盘分区。在安装操作系统时，将操作系统与应用系统安装在同一个磁盘分区，会导致一旦操作系统文件泄露时，攻击者可以通过操作系统漏洞获取应用系统的访问权限，从而影响应用系统的安全运行。
- 采用 FAT32 文件格式安装。FAT32 文件格式不能限制用户对文件的访问，会导致系统的不安全。
- 采用默认安装。默认安装操作系统时，会自动安装一些有安全隐患的组件，如

IIS、DHCP 和 DNS 等，导致系统在安装后存在多种安全漏洞。

• 系统补丁安装不及时不全面。在系统安装完成后，若不及时安装系统补丁程序，会导致病毒侵入。

2）运行隐患

在系统运行过程中，主要存在以下隐患：

• 默认共享。系统在运行后，会自动创建一些默认的共享：一是 C$、D$、E$ 每个分区的根共享目录；二是 ADMIN$ 远程管理用的共享目录；三是 IPC$ 空连接；四是 NetLogon 共享；五是其他系统默认共享，如 FAX$、PRINT$ 共享等。这些默认共享给系统的安全运行带来了很大的隐患。
• 默认服务。系统在运行后，自动启动了许多有安全隐患的服务，如 Telnet Services、DHCP Client、DNS Client、Print spooler、Remote Registry services、SNMP Services、Terminal Services 等。这些服务在实际工作中如不需要，可以将其禁用或关闭。
• 安全策略。系统运行后，默认情况下，系统的安全策略是不起作用的，这降低了系统的运行安全性。
• 管理员账号。系统在运行后，由于 Administrator 用户账号是不能停用的，导致攻击者可以一遍又一遍地尝试猜测这个账号的口令。此外，设置简单的用户账号口令也会给系统的运行带来安全隐患。
• 页面文件。页面文件是用来存储没有装入内存的程序和数据文件部分的隐藏文件。页面文件中可能含有一些敏感的资料，有可能造成系统信息的泄露。
• 共享文件。默认状态下，每个人对新创建的文件共享都拥有完全控制权限，这是非常危险的，应严格限制用户对共享文件的访问。
• Dump 文件。Dump 文件在系统崩溃和蓝屏的时候是一份很有用的查找问题的资料。然而，它也能够给攻击者提供一些敏感信息，比如一些应用程序的口令等，造成信息泄露。
• Web 服务。系统本身自带的 IIS 服务、FTP 服务存在安全隐患，容易导致系统成为攻击对象。

2. 安全防范对策

1）安装对策

在进行系统安装时，可采取以下对策：

• 在完全安装、配置好操作系统，并给系统全部安装系统补丁之前，一定不要把计算机接入网络。
• 在安装操作系统时，建议至少分 3 个磁盘分区。第 1 个分区用来安装操作系统，第 2 个分区存放 IIS、FTP 和各种应用程序，第 3 个分区存放重要的数据和日志文件。
• 采用 NTFS 文件格式安装操作系统，可以保证文件的安全，控制用户对文件的访问权限。
• 在安装系统组件时，不要采用默认安装，删除系统默认选中的 IIS、DHCP 和 DNS

等服务。

• 在安装完操作系统后，应先安装在其上面的应用系统，然后安装系统补丁。

2）运行对策

在系统运行时，可采取以下对策：

（1）关闭系统默认共享。

方法一，采用批处理文件在系统启动后自动删除共享。首选在 Cmd 提示符下输入 Net Share 命令，查看系统自动运行的所有共享目录。然后建立一个批处理文件 SHAREDEL.BAT，将该批处理文件放入计划任务中，并设置成每次开机时自动运行。文件内容如下：

```
NET SHARE C$        /DELETE
NET SHARE D$        /DELETE
NET SHARE E$        /DELETE
⋮
NET SHARE IPC$      /DELETE
NET SHARE ADMIN$    /DELETE
```

方法二，修改系统注册表，禁止默认共享功能。在 Local_Machine System CurrentControlSetServicesLanmanServerParameters 下新建一个双字节项 auto shareserver，将其值填为 0。

方法三，若要禁止这些共享，打开"管理工具"|"计算机管理"|"共享文件夹"|"共享"，在相应的共享文件夹上单击鼠标右键，选择"停止共享"即可。要注意的是，在机器重新启动后，这些共享又会重新自动开启。

（2）删除多余的不需要的网络协议。

删除网络协议中的 NWLink NetBIOS 协议、NWLink IPX/SPX/NetBIOS 协议和 NetBEUI PROtocol 协议和服务等，只保留 TCP/IP 网络通信协议。

（3）关闭不必要的有安全隐患的服务。

用户可以根据实际情况，关闭表 7-1 中所示的系统自动运行带有安全隐患的网络服务。

表 7-1 具有安全隐患的服务

服务名称	操作设置	服务名称	操作设置
DHCP Client	停止并禁用	SNMP Services	停止并禁用
DNS Client	停止并禁用	Telnet Services	禁用
Print spooler	停止并禁用	Terminal Services	禁用
Remote Registry Services	停止并禁用		

（4）启用安全策略。

安全策略包括以下 5 个方面：

• 账号锁定策略。设置账号锁定阈值，3～5 次无效登录后，即锁定账号。账号锁定

策略如表 7-2 所示。

表 7-2 账号锁定策略

策　略	设　置	策　略	设　置
复位账户锁定计数器	20min	账户锁定时间	20min
账户锁定阈值	3 次		

- 密码策略。一是密码必须符合复杂性要求;二是服务器密码长度最少设置为 8 个字符以上;三是密码最长保留期一般设置为 1～3 个月,即 30～90 天;四是密码最短存留期为 3 天;五是强制密码历史,记住的密码个数为 0;六是运行“为域中所有用户使用可还原的加密来储存密码”停用。密码策略如表 7-3 所示。

表 7-3 密码策略

策　略	设　置	策　略	设　置
密码复杂性要求	启用	强制密码历史	5 次
密码长度最小值	6 位	密码最长存留时间	42 天

- 审核策略。审核策略在系统默认安装时是关闭的。激活此功能有利于管理员很好地掌握机器的运行状态,有利于系统的入侵检测。可以从日志中了解到机器是否被人蛮力攻击、非法的文件访问等。开启安全审核是系统最基本的入侵检测方法。当攻击者尝试对用户的系统进行某些方式(如尝试用户口令、改变账号策略及未经许可的文件访问等)入侵的时候,都会被安全审核记录下来。避免不能及时察觉系统遭受的入侵以致系统遭到破坏。建议至少要开启审核登录事件、账户登录事件和账户管理 3 个事件。审核策略如表 7-4 所示。

表 7-4 审核策略

策　略	设　置	策　略	设　置
审核系统登录事件	成功/失败	审核策略更改	成功/失败
审核账户管理	成功/失败	审核特权使用	成功/失败
审核登录事件	成功/失败	审核系统事件	成功/失败
审核对象访问	成功/失败		

- “用户权利指派”。在“用户权利指派”中,将“从远端系统强制关机”权限设置为禁止任何人有此权限,防止黑客从远程关闭系统。
- “安全选项”。将“对匿名连接的额外限制”权限改为“不允许枚举 SAM 账号和共享”。也可以通过修改注册表中的值来禁止建立空连接,将 Local_Machine \System\CurrentControlSet\Control \LSA-RestrictAnonymous 的值改为 1。如在 LSA 目录下无该键值,可以新建一个双字节值,名为 restrictanonymous,值为 1,十六进制。此举可以有效地防止利用 IPC $ 空连接枚举 SAM 账号和共享资

源，造成系统信息的泄露。

(5) 加强对 Administrator 账号和 Guest 账号的管理监控。

将 Administrator 账号重新命名，创建一个陷阱账号，名为 Administrator，口令为 10 位以上的复杂口令，其权限设置成最低，即将其设为不隶属于任何一个组，并通过安全审核，借此发现攻击者的入侵企图。设置 2 个管理员用账号，一个具有一般权限，用来处理一些日常事物；另一个具有 Administrators 权限，只在需要的时候使用。修改增加 Guest 用户口令的复杂性，并禁用 Guest 用户账号。

(6) 禁止使用共享。

严格限制用户对共享目录和文件的访问，无特殊情况，严禁通过共享功能访问服务器。

(7) 清除页面文件。

将注册表 HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management 中 ClearPageFileAtShutdown 的值改为 1，可以禁止系统产生页面文件，防止信息泄露。

(8) 清除 Dump 文件。

依次选择“控制面板”|“系统属性”|“高级”|“启动和故障恢复”，将“写入调试信息”改成“无”，可以清除 Dump 文件，防止信息泄露。

(9) Web 服务安全设置。

若确需提供 Web 服务和 FTP 服务，可采取以下措施：

- IIS-Web 网站服务。在进行系统安装时不要安装 IIS 组件，系统安装完毕后，再手动添加该服务，将其安装目录名设为任意字符，以加大安全性。删除 Internet 服务管理器，删除样本页面和脚本，卸载 Internet 打印服务，删除除 ASP 外的应用程序映射。针对不同类型文件建立不同文件夹并设置不同权限。将脚本程序设为纯脚本执行许可权限，二进制执行文件设为脚本和可执行程序权限，静态文件设为读权限。对安全扫描出的 CGI 漏洞文件要及时删除。
- FTP 文件传输服务。不要使用系统自带的 FTP 服务，该服务与系统账户集成认证，一旦密码泄漏后果十分严重。建议利用第三方软件 SERV-U 提供 FTP 服务，该软件用户管理独立进行，并采用单向 Hash 函数(MD5)加密用户口令，加密后的口令保存在 ServUDaemon.ini 或是注册表中。用户采用多权限和模拟域进行权限管理。虚拟路径和物理路径可以随时变换。利用 IP 规则、用户权限、用户域和用户口令等多重保护防止非法入侵。

7.1.2 Windows 2000 Server 的安全设置

在这一小节中，从用户安全设置、密码安全设置、系统安全设置和服务安全设置这 4 个方面进行介绍。

1. 用户安全设置

1）禁用 Guest 账号

在计算机管理的用户里面把 Guest 账号禁用。为了保险起见，最好给 Guest 加一个复杂性的密码。可以打开记事本，在里面输入一串包含特殊字符、数字和字母的长字符串，然后把它作为 Guest 用户的密码复制进去。

2）限制不必要的用户

去掉所有的 Duplicate User 用户、测试用户和共享用户等。用户组策略设置相应权限，并且经常检查系统的用户，删除已经不再使用的用户。因为这些用户很多时候都是黑客们入侵系统的突破口。

3）创建两个管理员账号

创建一个一般权限用户用来收信以及处理一些日常事务，另一个拥有 Administrators 权限的用户只在特殊需要的时候使用。

4）将系统 Administrator 账号改名

因为 Windows 2000 Server 的 Administrator 用户是不能被停用的，攻击者可不断地尝试该用户密码进行攻击。尽量把它伪装成普通用户，比如改成 Guesycludx。

5）创建一个陷阱用户

创建一个名为 Administrator 的本地用户，把它的权限设置成最低，并且加上一个超过 10 位的超级复杂密码。该用户用以“诱骗”黑客来访问，借此发现黑客的入侵企图。

6）把共享文件的权限从 Everyone 组改成授权用户

任何时候都不要把共享文件的用户设置成 Everyone 组，包括打印共享。若默认的属性就是 Everyone 组，一定不要忘记修改。

7）开启用户策略

使用用户策略，分别设置复位用户锁定计数器时间为 20min，用户锁定时间为 20min，用户锁定阈值为 3 次。

8）禁止系统显示上次登录的用户名

默认情况下，登录对话框中会显示上次登录的用户名，这会使他人很容易获得系统的一些用户名。可以通过修改注册表的方法不让对话框里显示上次登录的用户名。具体方法为，打开注册表编辑器并找到注册表项“HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\Dont-DisplayLastUserName”，把 REG_SZ 的键值改成 1。

2. 密码安全设置

1）使用安全密码

一些公司的管理员创建账号的时候往往喜欢用公司名、计算机名做用户名，然后又把这些用户的密码设置得太简单，比如 welcome 等。因此，要注意密码的复杂性，还要记住经常更换密码。

2）设置屏幕保护密码

这是一个很简单也很有必要的操作。设置屏幕保护密码也是防止内部人员破坏服

务器的一个屏障。

3）开启密码策略

注意应用密码策略，如启用密码复杂性要求，设置密码长度最小值为 6 位 ，设置强制密码历史为 5 次，时间为 42 天(6 周)。

4）使用智能卡来代替密码

对于密码，总是使安全管理员进退两难，密码设置得过于简单容易受到黑客的攻击，密码设置太复杂又容易忘记。如果条件允许，用智能卡来代替复杂的密码是一个很好的解决方案。

3. 系统安全设置

1）使用 NTFS 格式分区

最好把服务器的所有分区都改成 NTFS 格式，NTFS 文件系统要比 FAT、FAT32 的文件系统安全得多。

2）运行防毒软件

杀毒软件不仅能杀掉一些著名的病毒，还能查杀大量木马和后门程序，因此要注意经常运行杀毒程序并升级病毒库。

3）下载最新的补丁程序

很多网络管理员没有访问安全站点的习惯，以至于一些漏洞都出现很久了，还留放着服务器的漏洞给非法用户攻击。一定要经常访问微软和一些安全站点，下载最新的 Service Pack 和漏洞补丁，是保障服务器长久安全的最佳方法。

4）锁住注册表

在 Windows 2000 Server 中，只有 Administrators 和 Backup Operators 才有从网络上访问注册表的权限，还可进一步设定注册表访问权限。

5）禁止用户从软盘和光驱启动系统

一些工具能通过引导系统来绕过原有的安全机制。如果用户的服务器对安全要求非常高，可以考虑使用可移动软盘和光驱。

6）利用 Windows 2000 Server 的安全配置工具来配置安全策略

微软提供了一套基于 MMC(管理控制台)安全配置和分析工具，利用它们可以很方便地配置用户的服务器以满足用户的要求。具体内容请参考微软主页 http://www.microsoft.com/windows2000/techinfo/howitworks/security/sctoolset.asp。

4. 服务安全设置

1）关闭不必要的端口

关闭端口意味着减少服务功能，在安全和服务方面需要作出折中决策。如果服务器安装在防火墙的后面，风险就会少得多，但并不意味着可以高枕无忧了。用端口扫描器扫描系统所开放的端口，确定开放了哪些服务是黑客入侵用户系统最常用的方法。在系统目录中的\system32\drivers\etc\services 文件中有知名端口和服务的对照表可供参考。具体方法为，依次选择“网上邻居”|“本地连接”|“属性”|“Internet 协议”|“TCP/IP”

|“属性”|“高级”|“选项”|“TCP/IP 筛选”|“属性”，打开“TCP/IP 筛选”，添加需要的TCP、UDP 协议即可。

2）设置好安全记录的访问权限

安全记录在默认情况下是不受到保护的，应把它设置成只有 Administrators 和系统账户才有权访问。

3）把敏感文件存放在另外的文件服务器中

虽然现在服务器的硬盘容量都很大，但还是应该考虑把一些重要的用户数据（文件、数据表和项目文件等）存放在另外一个安全的服务器中，并且经常备份它们。

7.1.3 Windows 2003 Server 的安全策略

1. 账户保护安全策略

用户账户的保护主要围绕着密码的保护来进行。为了避免用户身份由于密码的破解而被夺取或盗用，通常可采取诸如提高密码的破解难度、启用账户锁定策略、限制用户登录、限制外部连接以及防范网络嗅探等措施。

1）提高密码的破解难度

提高密码的破解难度主要是通过采用提高密码复杂性、增加密码长度及提高更换密码的频率等措施来实现，但这常常是用户很难做到的，对于企业网络中的一些安全敏感用户就必须采取一些相关的措施，以强制改变不安全密码的使用习惯。

在 Windows 系统中可以通过一系列的安全设置，并同时制定相应的安全策略来实现。在 Windows Server 2003 系统中，可以通过在安全策略中设定“密码策略”来设置。Window Server 2003 系统的安全策略可以根据网络的情况，针对不同的场合和范围有针对性地设置。例如可以针对本地计算机、域及相应的组织单元来设置，这完全取决于该策略要影响的范围。

以域安全策略为例，其作用范围是企业网中所指定域的所有成员。在域管理工具中运行“域安全策略”工具，然后就可以针对密码策略进行相应的设置。

密码策略也可以在指定的计算机上用“本地安全策略”来设定，同时也可在网络中特定的组织单元通过组策略进行设置。

2）启用账户锁定策略

账户锁定是指在某些情况下（例如账户受到采用密码词典或暴力猜测方式的在线自动登录攻击），为保护该账户的安全而将此账户锁定。使其在一定的时间内不能再次使用，从而挫败连续的猜测尝试。

Windows 2003 系统在默认情况下，为方便用户起见，这种锁定策略并没有进行设定，此时，对黑客的攻击没有任何限制。只要有耐心，通过自动登录工具和密码猜测字典进行攻击，甚至可以进行暴力模式的攻击，那么破解密码只是一个时间和运气的问题。账户锁定策略设定的第一步就是指定账户锁定的阈值，即锁定该账户无效登录的次数。一般来说，由于操作失误造成的登录失败的次数是有限的。在这里设置锁定阈值为 3 次，这样只允许 3 次登录尝试。如果 3 次登录全部失败，就会锁定该账户。

但是,一旦该账户被锁定后,即使是合法用户也就无法使用了。只有管理员才可以重新开启该账户,这就造成了许多不便。为方便用户,可以同时设定锁定的时间和复位计数器的时间。账户的锁定,可以有效地避免自动猜测工具的攻击,同时对于手动尝试者的耐心和信心也可造成很大的打击。锁定用户账户常常会造成一些不便,但系统的安全有时更为重要。

3) 限制用户登录

对于企业网的用户还可以通过对其登录行为进行限制,来保障用户账户的安全。这样限制以后,即使是密码出现泄漏,系统也可以在一定程度上将黑客阻挡在“门外”,对于Windows Server 2003 网络来说,运行“Active Directory 用户和计算机”管理工具。然后选择相应的用户,并设置其账户属性。

在账户属性对话框中,可以限制其登录的时间和地点。单击其中的“登录时间”按钮,在这里可以设置允许该用户登录的时间,这样就可防止非工作时间的登录行为。单击其中的“登录到”按钮,在这里可以设置允许该账户从哪些计算机登录。另外,还可以通过“账户”选项来限制登录时的行为。例如使用“用户必须用智能卡登录”,就可避免直接使用密码验证。除此之外,还可以引入指纹验证等更为严格的手段。

4) 限制外部连接

对于企业网络来说,通常需要为一些远程拨号的用户(业务人员或客户等)提供拨号接入服务。远程拨号访问技术实际上是通过低速的拨号连接来将远程计算机接入到企业内部的局域网中。由于这个连接无法隐藏,因此常常成为黑客入侵内部网络的最佳入口。但是,采取一定的措施可以有效地降低风险。

对于基于 Windows Server 2003 的远程访问服务器来说,默认情况下将允许具有拨入权限的所有用户建立连接。因此,安全防范的第一步就是合理地、严格地设置用户账户的拨入权限,严格限制拨入权限的分配范围。对于网络中的一些特殊用户和固定的分支机构的用户来说,可通过回拨技术来提高网络安全性。这里所谓的回拨,是指在主叫方通过验证后立即挂断线路,然后由被叫方回拨到主叫方的电话上。这样,即使账户及其密码被破解,也不必有任何担心。

在 Windows Server 2003 网络中,如果活动目录工作在 Native-mode(本机模式)下,这时就可以通过存储在访问服务器上或 Internet 验证服务器上的远程访问策略来管理。针对各种应用场景的不同,可以设置多种不同的策略。

5) 限制特权组成员

在 Windows Server 2003 网络中,还有一种非常有效的防范黑客入侵和管理疏忽的辅助手段,就是利用“受限制的组”安全策略。该策略可保证组成员的组成固定。在域安全策略的管理工具中添加要限制的组,在“组”对话框中输入或查找要添加的组。一般要对管理员组等特权组的成员加以限制。下一步就是要配置这个受限制的组的成员。在这里选择受限制的组的“安全性”选项。然后,就可以管理这个组的成员组成,可以添加或删除成员,当安全策略生效后,可防止黑客将后门账户添加到该组中。

6) 防范网络嗅探

由于局域网采用广播的方式进行通信,因而信息很容易被窃听。网络嗅探就是通过

侦听所在网络中所传输的数据来嗅探有价值的信息。对于普通的网络嗅探的防御并不困难，可通过以下手段来进行：

（1）采用交换网络。

一般情况下，交换网络对于普通的网络嗅探手段具有先天的免疫能力。这是由于在交换网络环境下，每一个交换端口就是一个独立的广播域，同时端口之间通过交换机进行桥接，而非广播。网络嗅探主要针对的是广播环境下的通信，因而在交换网络中就失去了作用。

随着交换网络技术的普及，网络嗅探所带来的威胁也越来越低，但仍不可忽视。通过 ARP 地址欺骗仍然可以实现一定范围的网络嗅探。

（2）加密会话。

在通信双方之间建立加密的会话连接也是非常有效的方法，特别是在企业网络中。这样，即使黑客成功地进行了网络嗅探，但由于捕获的都是密文，因而毫无价值。网络中进行会话加密的手段有很多，可以通过定制专门的通信加密程序来进行，但是通用性较差。因此，完善 IP 通信的安全机制才是最根本的解决办法。

由于历史原因，基于 IP 的网络通信技术没有内建的安全机制。随着互联网的发展，安全问题逐渐暴露出来。现在经过各个方面的努力，标准的安全架构也已经基本形成。那就是 IPSec 机制，并且它将作为下一代 IP 网络标准 IPv6 的重要组成。IPSec 机制在新一代的操作系统中已经得到了很好的支持。在 Windows Server 2003 系统中，其服务器产品和客户端产品都提供了对 IPSec 的支持。从而增强了安全性、可伸缩性以及可用性，同时使部署和管理更加方便。

在 Windows Server 2003 系统的安全策略相关的管理工具集（例如本地安全策略、域安全策略和组策略等）中，都集成了相关的管理工具。为清楚起见，可通过 Microsoft 管理控制台 MMC 定制的管理工具了解。

具体方法如下，首先在“开始”菜单中单击“运行”选项，然后输入 mmc，单击“确定”按钮。在“控制台”菜单中选择“添加删除管理单元”命令，然后，单击“添加”按钮。在可用的独立管理单元中，选择“IP 安全策略管理”选项，双击或单击“添加”按钮，在这里选择被该管理单元所管理的计算机，然后单击“完成”按钮。关闭添加管理单元的相关窗口，就得到了一个新的管理工具，在这里可以为其命名并保存。

此时可以看到已有的安全策略，用户可以根据情况来添加、修改和删除相应的 IP 安全策略。其中 Windows Server 2003 系统自带的有以下几个策略：

- 安全服务器（要求安全设置）；
- 客户端（只响应）；
- 服务器（请求安全设置）。

其中的“客户端”策略是根据对方的要求来决定是否采用 IPSec；“服务器”策略要求支持 IP 安全机制的客户端使用 IPSec，但允许不支持 IP 安全机制的客户端来建立不安全的连接；而“安全服务器”策略则最为严格，它要求双方必须使用 IPSec 协议。

不过，“安全服务器”策略默认允许不加密的受信任的通信，因此仍然能够被窃听。直接修改此策略或定制专门的策略，就可以实现有效的防范。选择其中的“所有 IP 通

信”选项，在这里可以编辑其规则属性。

选择“筛选器操作”选项卡，选择其中的“要求安全设置”选项。

2. 系统监控安全策略

尽管不断地在对系统进行修补，但由于软件系统的复杂性，安全漏洞问题仍然存在。因此，除了对安全漏洞进行修补之外，还要对系统的运行状态进行实时监视，以便及时发现利用各种漏洞的入侵行为。如果已有安全漏洞但还没有全部得到修补，这种监视就显得尤其重要。

1）启用系统审核机制

系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员进行分析、查找系统和应用程序故障以及各类安全事件。

所有的操作系统、应用系统等都带有日志功能，因此可以根据需要实时地将发生在系统中的事件记录下来。同时还可以通过查看与安全相关的日志文件的内容，发现黑客的入侵行为。当然，若要达到这个目的，就必须具备一些相关的知识。首先必须要学会如何配置系统，以启用相应的审核机制，并同时使之能够记录各种安全事件。

对 Windows Server 2003 的服务器和工作站来说，为了不影响系统性能，默认的安全策略并不对安全事件进行审核。从“安全配置和分析”工具用 SecEdit 安全模板进行的分析结果可知，有红色标记的审核策略应该已经启用，这可用来发现来自外部和内部的黑客入侵行为。对于关键的应用服务器和文件服务器来说，应同时启用剩下的安全策略。

如果已经启用了“审核对象访问”策略，那么就要求必须使用 NTFS 文件系统。NTFS 文件系统不仅提供对用户的访问控制，而且还可以对用户的访问操作进行审核。但这种审核功能，需要针对具体的对象来进行相应的配置。

首先在被审核对象“安全”属性的“高级”属性中添加要审核的用户和组。在该对话框中选择好要审核的用户后，就可以设置对其进行审核的事件和结果。在所有的审核策略生效后，就可以通过检查系统的日志来发现黑客的蛛丝马迹。

2）日志监视

在系统中启用安全审核策略后，管理员应经常查看安全日志的记录，否则就失去了及时补救和防御的时机。除了安全日志外，管理员还要注意检查各种服务或应用的日志文件。在 Windows 2003 IIS 6.0 中，其日志功能默认已经启动，并且日志文件存放的路径默认在 System32/LogFiles 目录下，打开 IIS 日志文件，可以看到对 Web 服务器的 HTTP 请求，IIS 6.0 系统自带的日志功能从某种程度上可以成为入侵检测的得力助手。

3）监视开放的端口和连接

对日志的监视只能发现已经发生的入侵事件，但是它对正在进行的入侵和破坏行为是无能为力的。这时，就需要管理员掌握一些基本的实时监视技术。

通常在系统被黑客或病毒入侵后，就会在系统中留下木马类后门。同时它和外界的通信会建立一个 Socket 会话连接，可用 netstat 命令进行会话状态的检查，可以查看已经打开的端口和已经建立的连接。当然也可以采用一些专用的检测程序对端口和连接进行检测。

4）监视共享

通过共享来入侵一个系统不失为一种方便的手段，最简单的方法就是利用系统隐含的管理共享。因此，只要是黑客能够扫描到的 IP 和用户密码，就可以使用 net use 命令连接到共享上。另外，当浏览到含有恶意脚本的网页时，计算机的硬盘也可能被共享，因此，监测本机的共享连接是非常重要的。

监测本机的共享连接具体方法如下，在 Windows Server 2003 的计算机中，打开“计算机管理”工具，并展开“共享文件夹”选项。单击其中的“共享”选项，就可以查看其右面窗口，以检查是否有新的可疑共享，如果有可疑共享，就应该立即删除。另外，还可以通过选择“会话”选项，来查看连接到机器所有共享的会话。Windows NT/2000 的 IPC $ 共享漏洞是目前危害最大的漏洞之一。黑客即使没有马上破解其密码，也仍然可以通过“空连接”来连接到系统上，再进行其他的尝试。

5）监视进程和系统信息

对于木马和远程监控程序，除了监视开放的端口外，还应通过任务管理器的进程查看功能进行进程的查找。在安装 Windows Server 2003 的支持工具（从产品光盘安装）后，就可以获得一个进程查看工具 Process Viewer；通常，隐藏的进程寄宿在其他进程下，因此查看进程的内存映象也许能发现异常。但是，现在的木马越来越难发现，它常常会把自己注册成一个服务，从而避免了在进程列表中现形。因此，还应结合对系统中的其他信息的监视，这样就可对系统信息中的软件环境下的各项进行相应的检查。

7.1.4 Windows Server 2003 防火墙

“冲击波”等蠕虫病毒特征之一就是利用有漏洞的操作系统进行端口攻击，因此防范此类病毒的简单方法就是屏蔽不必要的端口，防火墙软件都具有这种功能，其实对于采用 Windows 2003 或者 Windows XP 的用户来说，不需要安装任何其他软件，因为可以利用系统自带的“Internet 连接防火墙”来防范黑客的攻击。

1. 基本设置

- 右击“网上邻居”，选择“属性”命令。
- 然后右击“本地连接”，选择“属性”命令，出现如图 7-1 所示的界面。选择“高级”选项，选中“Internet 连接防火墙”，确定后防火墙即起作用。

2. 测试基本设置

- 在另外一台机器上 ping 本机，出现 Request timed out 表示 ping 不通本机。
- 在另外一台机器上用漏洞扫描工具扫描本机发现没有打开的端口。

这两种测试通过后也说明防火墙已经起作用。

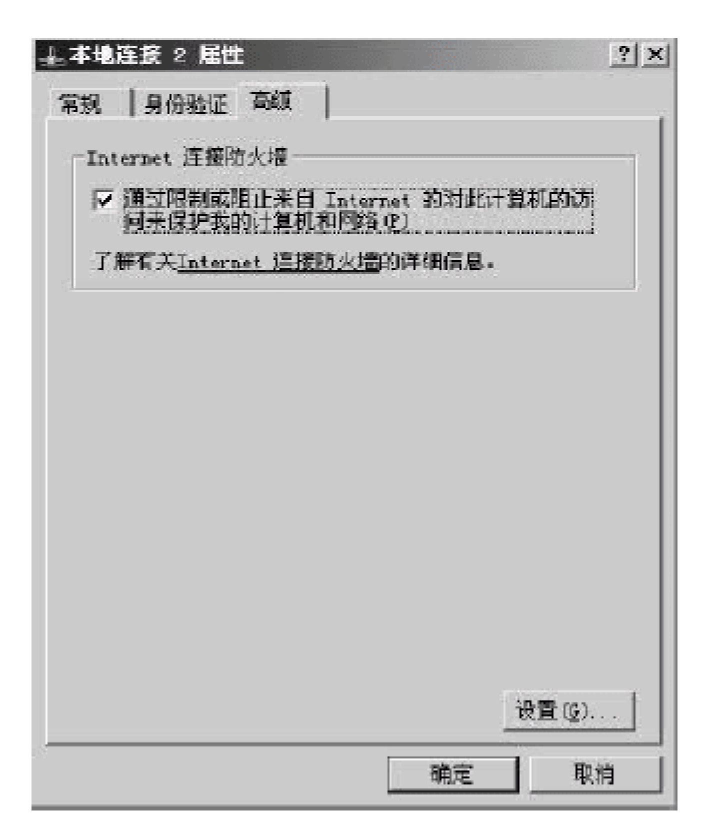


图 7-1　本地连接属性

3. 高级设置

单击图 7-1 中“设置…”按钮，出现如图 7-2 所示的界面后，则可进行高级设置。

1）选择要开通的服务

如图 7-3 所示，如果本机要开通相应的服务，可选中该服务，本例选中了 FTP 服务，这样从其他机器就可 FTP 到本机，扫描本机可以发现 21 端口是开放的。可以单击“添加”按钮增加相应的服务端口。



图 7-2 高级设置主窗口



图 7-3 服务开通设置

2）设置日志

如图 7-4 所示，选择要记录的项目，防火墙将记录相应的数据，日志默认在 c：\windows\pfirewall. log，其内容用“记事本”就可以打开查看。

3）设置 ICMP 协议

如图 7-5 所示，最常用的 ping 就是用的 ICMP 协议，默认设置完后 ping 不通本机就是因为屏蔽了 ICMP 协议，如果想 ping 通本机只需选中“允许传入响应请求”项即可（即在该选项前打一个“√”）。



图 7-4 日志设置

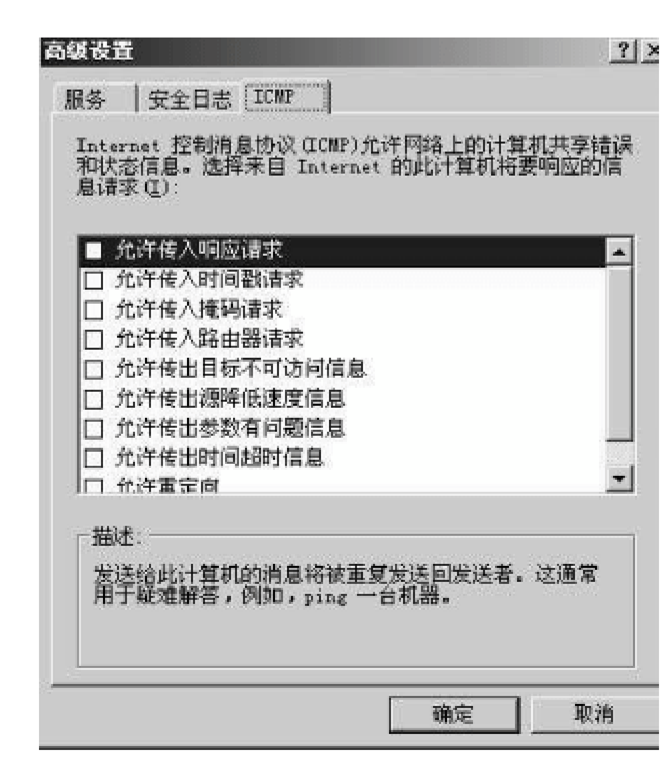


图 7-5 ICMP 设置

7.2 UNIX安全

UNIX/Linux 是适用于多种硬件平台的多用户、多任务操作系统，其安全性是很高的。系统提供了 3 层的防御体系，账号安全、权限设置和文件系统安全。下面分别对这 3 个方面进行阐述。

由于 Linux 是一种与 UNIX 安全兼容的操作系统，所以下面所讨论的 UNIX 系统的安全性问题，基本上也适用于 Linux 系统。

7.2.1 UNIX安全概述

1. 用户账号和口令

1）默认账号。所有的 UNIX 系统安装完毕后都有默认账号，有时这些账号有默认的口令或者根本没有口令，这样，它们就成为攻击者最好的突破口。所以，安装完后，系统管理员一定要及时修改系统账号及其登录口令。

2）共享账号。UNIX 系统的每个用户都应该有自己的专用账号。如果允许用户使用共享，即多个用户使用相同的账号，该账号的安全性就被破坏了。

3）口令安全。用户的口令是对系统安全的最大安全威胁。如果入侵者获得一个用户的口令，那他就可以轻易地登录到系统上，并且拥有这个用户的所有权限。任何登录 UNIX 系统的人，都必须输入口令，而口令文件只有超级用户可以读写。攻击者的目的主要是通过破解口令文件，寻找出口令，从而可以冒充合法用户访问主机，因此一旦用户发现系统的口令文件被非法访问过，一定要及时更换所有的用户口令。

安全口令应有以下几个特点。

- 位数大于 6 位，最好是 8 位以上。
- 大小写字母混合。如果有一个大写字母，不要放在开头。
- 如果记忆较好，可以把数字无序地加在字母中。
- 当口令中有“-！ @＃＄％&＊<>”等特殊符号时，不要放在结尾。

不安全的口令则有以下几种情况。

- 使用用户名（账号）作为口令或使用用户名（账号）为变换形式作为口令。
- 使用自己或者亲友的生日作为口令。
- 使用常用的英文单词作为口令。
- 使用 5 位或 5 位以下的字符作为口令。

实际上 UNIX 的口令设计是十分完善的，一般用户不可能把自己的密码改成用户名、小于 4 位或简单的英文单词。这是 UNIX 系统默认的安全模式，是除了系统管理员（超级用户）以外不可改变的。因此，安装 UNIX 后只要更改初始的 root 口令。

尽管如此，黑客还是能通过其他途径获得口令，主要有两种途径。

- 利用技术漏洞。如缓冲区溢出，send mail 漏洞、finger、AIX 的 rlogin 等。
- 利用管理漏洞。如 root 身份运行 http、建立 shadow 的备份但是忘记更改其属性、用电子邮件寄送密码等。

2. 用户和用户组

虽然每个 UNIX 用户都有一个长达 8 个字符以上的用户名，但在 UNIX/Linux 内部只用一个数字来标识每个用户，用户的标识符(UID)。通常，系统为每一个用户分配一个不同的 UID。

UID 被规定为一个无符号的 16 位整数，这意味着其取值范围是 0～65 535。

UID 是操作系统用于识别用户的实际信息，系统提供用户名仅仅是出于方便用户考虑。如果两个用户被分配给相同的 UID，系统将他们视为同一个用户，即使他们有不同的用户名和口令也是如此。特别要注意的是，两个具有相同 UID 的用户可以自由地读取和删除对方的文件。

出于管理的方便，UNIX/Linux 系统还划分了用户组，每个用户都位于一个或者多个用户组中。与用户标识一样，每一个用户组在系统内部也用了一个整数标识，称为用户组标识(GID)。

每一个 UNIX/Linux 系统都有一个 UID 为 0 的特殊用户，它被称作超级用户并且被赋予用户名 root，其口令通常称为"root 口令"。

UNIX 系统管理员经常需要用超级用户去执行各种系统管理任务。这可以通过 Su 命令建立一个特权 Shell 来实现。执行超级用户的操作必须格外小心。当超级用户的操作执行完毕，系统管理员应该从这个特权 shell 中退出。

在前面提到，用户名在系统内部是以用户标识来表示的。两个 UID 相同的用户名在系统看来是同一个用户，因此，任何 UID 为 0 的用户都是超级用户。用户名 root 仅仅是一个通常的约定。

很多 UNIX/Linux 系统可以配置为禁止远程终端登录。任何想具有超级用户权限的用户，必须首先登录到自己的账户，然后，再通过 su 命令进入 root 账号。这个特点使得对那些使用 root 账户的用户跟踪变得容易，因为 su 命令记录了调用它的用户名以及调用时间。这个特点也增加了系统的安全度，因为登录者必须知道两个口令才能得到超级用户的特权。

7.2.2 UNIX 安全性分析

1. 口令安全

UNIX 系统中的/etc/passwd 文件含有每个用户的所有信息(加密后的口令可存于/etc/shadow 文件中)。

/etc/passwd 中包含有用户的登录名、经过加密的口令、用户号、用户组号、用户注释、用户主目录和用户所用的 shell 程序。其中用户号(UID)和用户组号(GID)用于 UNIX 系统唯一地标识用户和同组用户及用户的访问权限。

/etc/passwd 中存放的加密口令用于用户登录时输入的口令经计算后相比较，符合则允许登录，否则拒绝用户登录。用户可用 passwd 命令修改自己的口令，但不能直接修改/etc/passwd 中的口令。

一个优秀的口令至少应有 8 个字符长，不要用个人信息(如生日、姓名、反向拼写的登录名和机房中可见的物品等)、普通的英语单词作为口令，口令中最好有一些非字母(如数字、标点符号和控制字符等)，还要便于记忆，不能写在纸上或计算机中的文件中，选择口令的一个好方法是将两个不相关的词用一个数字或控制字符相连，并截断为 8 个字符。当然，如果你能记住 8 位乱码更好。

不应将同一个口令在不同机器中使用，特别是在不同级别的用户上使用同一口令，否则会引起全盘崩溃。用户应定期改变口令，至少 3 个月要改变一次，系统管理员可以强制用户定期做口令修改。

为防止眼明手快的人窃取口令，在输入口令时应确认无人在身边。

2. 文件许可权

文件属性决定了文件的被访问权限，即谁能存取或执行该文件。用 ls -l 可以列出详细的文件信息，如：

```
- rwxrwxrwx  1  pat  cs440  70  Jul  28  21:12  zombin
```

包括了文件许可、文件联结数、文件所有者名、文件相关组名、文件长度、上次存取日期和文件名。

其中文件许可分为 4 部分。

符号“-”。表示文件类型。

第一个 rwx。表示文件属主的访问权限。

第二个 rwx。表示文件同组用户的访问权限。

第三个 rwx。表示其他用户的访问权限。

若某种许可被限制则相应的字母换为“-”。

在许可权限的执行许可位置上，可能是其他字母 s，S，t，T。s 和 S 可出现在所有者和同组用户许可模式位置上，与特殊的许可有关，下面将讨论。t 和 T 可出现在其他用户的许可模式位置上，与“粘贴位”有关而与安全无关。小写字母(x，s，t)表示执行许可为允许，负号或大写字母(-，S 或 T)表示执行许可为不允许。

改变许可方式可使用 chmod 命令，并以新许可方式和该文件名为参数。新许可方式以 3 位 8 进制数给出，r 为 4，w 为 2，x 为 1。如 rwxr-xr--为 754。

chmod 也有其他方式的参数可直接对某组参数修改，详见 UNIX 系统的联机手册。

文件许可权可用于防止偶然性地重写或删除一个重要文件(即使是属主自己)。

改变文件的属主和组名可用 chown 和 chgrp 命令，但修改后原属主和组员就无法修改回来。

3. 目录许可

在 UNIX 系统中，目录也是一个文件，用 ls -l 列出时，目录文件的属性前面带一个 d，目录许可也类似于文件许可，用 ls 列目录要有读许可，在目录中增删文件要有写许可，进入目录或将该目录作路径分量时要有执行许可。因此，若要使用一个文件，必须具有

该文件及找到该文件的路径上所有目录分量的相应许可。仅当要打开一个文件时，文件的许可才开始起作用，而 rm、mv 只需要有目录的搜索和写许可，而不需文件的许可，这一点应注意。

4. umask 命令

umask 设置用户文件和目录的文件创建默认屏蔽值，若将此命令放入.profile 文件，就可控制该用户后续所建文件的存取许可.umask 命令与 chmod 命令的作用正好相反，它告诉系统在创建文件时不给予什么样的存取许可。

5. 设置用户 ID 和同组用户 ID

用户 ID 许可(SUID)和同组用户 ID 许可(SGID)可给赋予可执行的目标文件，因为只有可执行文件才有意义，当一个进程执行时就被赋予 4 个编号，以标识该进程隶属于谁，分别为实际和有效的 UID，实际和有效的 GID。有效的 UID 和 GID 一般和实际的 UID 和 GID 相同，有效的 UID 和 GID 用于系统确定该进程对于文件的存取许可。而设置可执行文件的 SUID 许可将改变上述情况，当设置了 SUID 时，进程的有效 UID 为该可执行文件的所有者的有效 UID，而不是执行该程序的用户的有效 UID，因此，由该程序创建的都有与该程序所有者相同的存取许可。这样，程序的所有者将可通过程序的控制在有限的范围内向用户发布不允许被公众访问的信息。同样，SGID 是设置有效 GID。可用 chmod u+s 文件名和 chmod u−s 文件名来设置和取消 SUID 设置，用 chmod g+s 文件名和 chmod g−s 文件名来设置和取消 SGID 设置。当文件设置了 SUID 和 SGID 后，chown 和 chgrp 命令将全部取消这些许可。

6. su 和 newgrp 命令

1）su 命令

UNIX 系统允许在不注销用户的情况下而允许另一用户登录进入系统，新登录的用户将启动新的 shell，并将有效和实际的 UID 和 GID 设置给该用户，因此必须严格将 root 口令保密。

2）newgrp 命令

与 su 相似，用于修改当前组名。

7. 文件加密

crypt 命令可提供给用户用以加密文件，使用一个关键词将标准输入的信息编码为不可读的杂乱字符串，送到标准输出设备。再次使用该命令，用同一关键词作用于加密后的文件，可恢复文件内容。一般来说，在文件加密后，应删除原始文件，只留下加密后的版本，且不能忘记加密关键词。在 vi 中一般都有加密功能，用 vi −x 命令可编辑加密后的文件。关于加密关键词的选取规则与口令的选取规则相同。由于 crypt 程序可能被做成特洛依木马，故不宜用口令作为关键词。最好在加密前用 pack 或 compress 命令对文件进行压缩后再加密。

7.23 UNIX安全体系结构

UNIX 的安全体系结构可以按照 ISO/OSI 网络模型的层次结构将它分成 7 层，如表 7-5 所示。

表 7-5　UNIX 安全体系结构

层　次	名　称	含　义
7	Policy	安全策略定义、指导
6	Personnel	使用设备和数据的人员
5	LAN	计算机设备和数据
4	Internal Demark	内部区分
3	Gateway	OSI 中第 7、6、5、4 层的功能
2	Packet-Filter	OSI 中第 3、2、1 层的功能
1	External Demar	外部连接

1. External Demark（外部连接层）

外部连接层定义用户系统如何与设备、电话线路或其他用户不能直接控制的介质进行连接。完整的用户安全策略应包括这一部分，因线路本身可允许非授权访问。

2. Packet-Filter（包过滤层）

它对应于 OSI 的第 1 层到第 3 层，本层不仅提供第 1 层的物理连接，更主要的是根据安全策略，通过用户层的进程和包过滤规则对网络层中的 IP 包进行过滤。一般的包过滤算法是采用查规则表来实现的，它根据“条件/动作”的规则序列来判断是将包传给路由还是将包丢弃。

3. Gateway（嵌入的 UNIX 网关层）

嵌入的 UNIX 网关层定义了整体平台包括第 4 层的网络接口以及第 3 层的路由器。它用于为广域网提供防火墙服务。

4. Internal Demark（内部区分层）

内部区分层定义了用户如何将局域网连接到广域网以及如何将局域网连接到防火墙上。

5. LAN(局域网层）

局域网层定义用户的安全程序要保护的设备和数据，包括计算机互联设备。如路由器、单一的 UNIX 主机等。

6. Personnel（用户层）

用户层定义了 UNIX 的安装、操作、维护、使用以及通过其他方法访问网络的人员。从广义上讲，对 UNIX 多用户环境下的应用进程也应算在其中。这一层的安全策略应该反映出用户对总体系统安全的期望值。

7. Policy（策略层）

策略层主要定义组织的安全策略，包括安全策略的需求分析、安全方针的制定。

7.2.4 保障 UNIX 安全的具体措施

1. 防止缓冲区溢出

据统计，约 80%以上的安全问题来自缓冲区溢出。攻击者通过写一个超过缓冲区长度的字符串，然后植入到缓冲区，可能会出现两个结果，一是过长的字符串覆盖了相邻的存储单元，引起程序运行失败，严重的可导致系统崩溃；另有一个结果就是利用这种漏洞可以执行任意指令，甚至可以取得系统 root 特级权限。一些版本的 UNIX 系统（如 Solaris 2.6 和 Solaris 7）具备把用户堆栈设成不可执行的功能，以使这种攻击不能得逞。以下是具体步骤。

- 进入 root 目录。
- 对/etc/system 文件做个备份 cp /etc/system /etc/system.BACKUP。
- 用编辑器编辑/etc/system 文件。
- 到文件的最后，插入以下几行：

```
set noexec_user_stack=1
set noexec_user_stack_log=15
```

保存文件，退出编辑器后，重启计算机，以使这些改变生效。但要注意可能有些合法使用可执行堆栈的程序在做如上改变后不能正常运行。

2. 在 inetd.conf 中关闭不用的服务

UNIX 系统中有许多用不着的服务自动处于激活状态。有部分服务存在的安全漏洞会使攻击者根本不需要账户就能控制机器。为了系统的安全，应把不用的功能关闭，以限制的文件限制访问权限。可以用以下方法来关闭。

（1）进入 root 目录。

（2）备份 inetd 的配置文件/etc/inetd.conf，即：

```
cp  /etc/inetd.conf  /etc/inetd.conf.BACKUP
```

（3）编辑/etc/inetd.conf 文件。

以“#”符号注释掉不需要的服务，使其处于不激活的状态。在需要很高安全性的机器上，最好注释掉 Telnet 和 FTP，即使要使用此两项服务，也要对使用情况进行限制，如

用 TCP Wrapper 对使用 Telnet 或 FTP 的 IP 地址进行限制。

(4) 在改变/etc/inetd.conf 后，找到 inetd 进程的 ID 号，用 kill 向它发送 HUP 信号来刷新。一定要确保 kill 了 inetd 进程后，它仍旧在运行。

3. 给系统打补丁

UNIX 系统被发现的漏洞，几乎都有了相应的补丁程序。因此，系统管理员需对系统漏洞做及时的修补。

4. 重要主机单独设立网段

从安全角度考虑，应当将重要机密信息应用的主机单独设立一个网段，以避免某一台计算机被攻破时，造成整个系统全部暴露。

5. 定期检查

定期检查系统日志文件，在备份设备上及时备份。定期检查关键配置文件(最长不超过 1 个月)。

重要用户的口令应该定期修改(不长于 3 个月)，严格要求不同主机使用不同的口令。

7.3 应用实例

7.3.1 Windows 98 屏保口令的破解与保护技术

利用 Windows 98 系统的屏幕保护功能可以有效地防止他人在自己不在的情况下偷用自己的计算机，从而起到安全保护的作用。不过在不配合其他限制功能的情况下，系统的屏幕保护是非常脆弱的。在遗忘了密码之后，只需使用“复位(REST)”按钮强行启动计算机，然后，右击桌面空白处并从弹出的快捷菜单中执行“属性”命令，打开“显示属性”设置对话框并单击“屏幕保护”选择项，最后取消“密码保护”选项即可。

若计算机有登录限制，则破解屏幕保护密码要困难些，可采用以下几种方法。

1. 利用网络破解

在计算机局域网内利用另一台计算机作为解码机，首先将解码机的 IP 地址改为需要破解计算机的 IP 地址，利用硬件冲突优先的原理就可以使 Windows 98 跳过屏幕保护程序。

当解码机修改 IP 地址并重新启动后，在需要破解屏幕保护程序的计算机上会出现“IP 地址硬件冲突”的提示框，单击“确定”按钮后，系统不要求输入屏幕保护的密码就能直接进入 Windows 98 桌面。

2. 利用光盘的自动运行特性(autorun)破解

若光盘上带有 Autorun.inf 文件，插入这张光盘后，光驱就会自动启动。其运行程序

就是 Autorun.inf 文件上“open=”后指定的程序。该程序运行完毕，自动回到 Windows 98 桌面。

3. 防护措施

防止这种攻击的有效手段是禁止光盘的 Autorun 特性。

- 从控制面板上打开“系统”。
- 选择“设备管理器”。
- 展开 CDROM 选项，双击 COROM 选项下的设备名，如图 7-6 所示。
- 选择“设置”选项卡，取消选中“自动插入通告”复选框，如图 7-7 所示。



图 7-6 系统属性

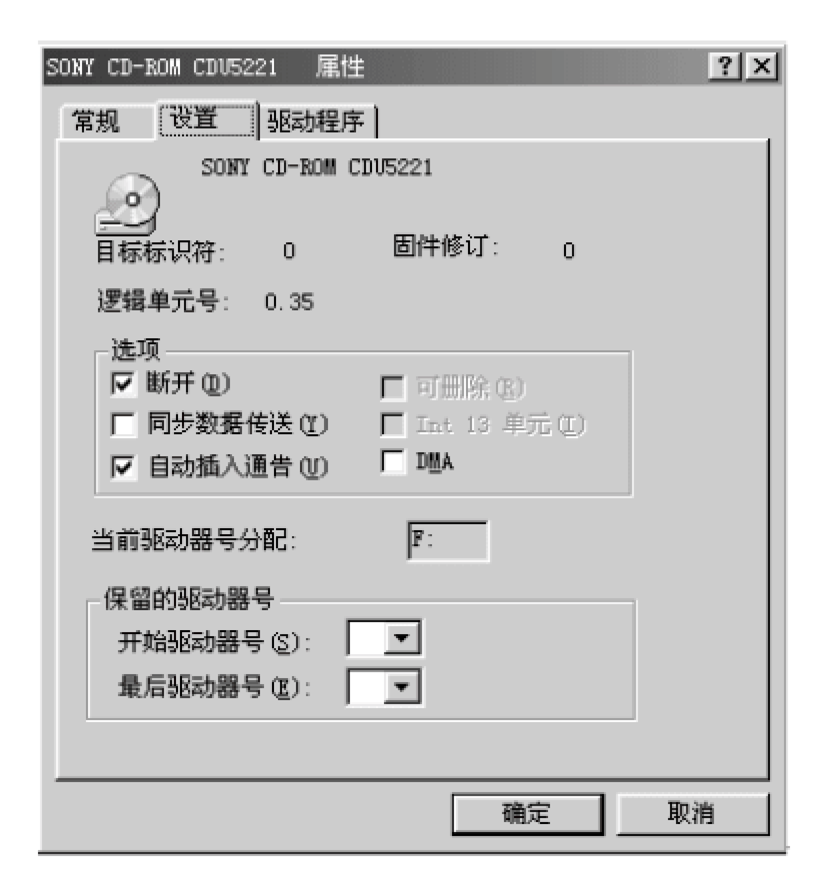


图 7-7 CD-ROM 设置

7.3.2 注册表修复技术

本小节介绍 Windows 2000 的注册表的修复技术，该技术可作为其他版本 Windows 系统注册表修复的参考。

1. 屏蔽“控制面板”中的指定项目

屏蔽“控制面板”中的某些项目，以防止用户进行任意设置。新建一个双字节(REG_DWORD)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowCpl，修改其值为 1。然后新建一个注册表项 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowCpl，在该项下新建若干个字符串(REG_SZ)值项，形式为“序号=控制面板项对应的文件名”。如想屏蔽控制面板中的“显示”和“系统”两项，可以在该项下新建两个值项 1 和 2，值分别为“desk.cpl”(显示项对应的文件)和 sysdm.cpl(系统项对应的文件)。重启计算机更改生效。

2. 指定“控制面板”中显示的项目

在“控制面板”中只显示指定的项目，对于没有指定的项目则不显示。新建一个双字节(REG_DWORD)类型的值项 HKEY_CURRENT_USER\Software\ Microsoft\Windows\Current Version\Policies\Explore\RestrictCpl，修改其值为 1，然后新建一个注册表项 HKEY_CURRENT_USER\ Software \ Microsoft \ Windows \ Current Version \ Policies \ Explore\RestrictCpl，在该项下新建若干个字符串(REG_SZ)值项，形式为“序号＝控制面板项对应的文件名”。如只允许用户使用控制面板中的“显示”和“系统”两项，可以在该项下新建两个值项 1 和 2，值分别为“desk. cpl”和 sysdm. cpl。重启计算机更改生效。

注意，使用“屏蔽控制面板中的指定项目”和“指定控制面板中显示的项目”都可以定制控制面板中项目的显示，但是这两个方法有可能发生冲突。如果发生冲突，则“屏蔽控制面板中的指定项目”设置优先。

3. 禁用控制面板中的“显示”项

禁止使用“控制面板”中的显示项。虽然该项仍然会出现在“控制面板”中，但是却不能使用。新建一个双字节(REG_DWORD)的值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\System\NoDispCPL，修改其值为 1。这时进入“控制面板”，双击“显示”项，系统会出现一个消息框提示用户不可以进行此操作。重启计算机更改生效。

4. 屏蔽“显示”项中的“背景”选项卡

通过屏蔽“背景”选项卡，可以避免用户更改桌面的墙纸。新建一个双字节值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\system\NoDispBackgr oundPage，修改其值为 1。重启计算机更改生效。

5. 禁止“显示”项里的“背景”选项卡

通过禁止“显示”项里的“背景”选项卡，“背景”页中的各个按钮和选择项都变成不可选状态，这样用户将无法更改当前的墙纸和背景。新建一个双字节值项 HKEY_CURRENT _ USER \ Software \ Microsoft \ Windows \ Current Version \ Policies \ ActiveDesktop\No ChangingWallPaper，修改其值为 1。重启计算机更改生效。

6. 屏蔽“显示”项中的“外观”选项卡

新建一个双字节(REG_DWORD)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\system\NoDispAppearancePage，修改其值为 1。重启计算机更改生效。

7. 禁止在“打印机”项中删除打印机

新建一个双字节(REG_DWORD)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer\NoDeletePrinter，修改其值为 1。这时进入“控

制面板”，选定一个打印机，右击，选择快捷菜单中的“删除”，系统会弹出一个消息框，提示用户不能进行删除打印机的操作。

8. 屏蔽“打印机”中的“添加打印机”

可以去除“打印机”项中的“添加打印机”，以防止用户任意配置新的打印机。新建一个字符串(REG_SZ)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer\NoAddPrinter，修改其值为 1。重启计算机更改生效。

9. 屏蔽“添加/删除”项

通过“控制面板”中的“添加/删除”项，用户可以安装和卸载 Windows 2000 的应用程序，还可以添加和删除 Windows 2000 的功能组件。

新建一个字符串(REG_SZ)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Uninstall\NoAddRemovePrograms，修改其值为 1。这时再进入到“控制面板”中，可以看到“添加/删除”图标不见了。

10. 屏蔽“添加/删除”项中的“更改或删除程序”选项

可以屏蔽掉“添加/删除”项中的“更改或删除程序”阻止用户更改或删除程序。新建一个双字节(REG_DWORD)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall\NoRemovePage，修改其值为 1。刷新桌面使更改生效。

11. 屏蔽“添加/删除”项中的“添加新程序”

可以通过屏蔽掉“添加/删除”项中的“添加新程序”以阻止用户添加新程序。新建一个双字节(REG_DWORD)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Uninstall\NoAddPage，修改其值为 1。

12. 屏蔽“添加/删除”项中的“添加/删除 Windows 组件”

可以屏蔽掉“添加/删除”项中的“添加/删除 Windows 组件”。使用户不能通过“添加/删除”项中的“添加/删除 Windows 组件”安装新的 Windows 2000 应用程序。新建一个双字节(REG_DWORD)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Uninstall\NoWindowsSetupPage，修改其值为 1。

13. 屏蔽“添加/删除”项目“添加新程序”中的“从光盘或软盘添加程序”

通过“添加/删除”项中的“添加新程序”，用户可以安装新的 Windows 2000 应用程序。可以去除掉“从光盘或软盘添加程序”方式。新建一个双字节(REG_DWORD)值项 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\Uninstall\NoAddFromCDor Floppy，修改其值为 1。

14. 优化 CDROM 预读取性能

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\CDFS 下，新建项 Prefetch(dword 类型)，根据 CDROM 的速度来给 Prefetch 赋值。

16 倍速：00000380 24 倍速：00000540

32 倍速：00000700 36 倍速：00000750

40 倍速：00000000 48 倍速：00000000

如果改后 CDROM 工作不正常，则降低一个级别赋值。

15. 提高软驱读写缓冲性能

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Class\fdc\0000 下，新增项 ForceFIFO(dword 类型)，设置键值为 1。

16. 优化文件系统

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem 下，新增项 ConfigFileAllocSize(dword 类型)，设置键值为 000001f4。

17. 删除不必要的自启动程序

在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下，删除不必要的自启动程序对应的键值。有些程序也可能藏在 Run 项下的 SysExpl 子项下，如有该子项，将其中的键值删除，同样也能取消自启动程序。

18. 卸载不用的应用软件

在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall 下，新建应用软件子项，然后在该子项中，新建项 DisplayName(REG_SZ 类型，值为"软件文件名")和 UninstallString(REG_SZ 类型，值为带路径的"反安装程序文件名")。

19. 删除软件残骸垃圾

有些程序卸载后还有注册信息留在注册表内，时间一长，这种垃圾愈来愈多，影响机器运行速度和效率。应经常进入 HKEY_LOCAL_MACHINE\Software、HKEY_CURRENT_USER\Software、HKEY_USERS \Default\Software 下，查找并删除这些垃圾。

20. 自动登录系统

在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current-Version\Winlogon 下，修改 AutoAdminLogon 项，键值为 1，表示自动登录；键值为 0 显示登录窗口，然后手工登录。

21. 禁止活动桌面功能

在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 下，新增项 NoActiveDesktop(dword 类型)，键值为“hex：01000000”，表示禁止活动桌面功能；为 0 表示启用。

22. 清理在桌面上右击弹出的菜单中的“新建”命令

在 HKEY_CLASSES_ROOT 和 HKEY_LOCAL_MACHINE 下，从左边的两个主项中，搜索 shellnew 并把该子项删除即可。

23. 清除配色方案

在 HKEY_CURRENT_USER\Control Panel\Appearance\Schemes 下，窗口右边会出现系统自带的各种配色方案，将自己认为无用的配色方案删除，一般只保留“Windows 默认”一项。

24. 加速菜单显示

在 HKEY_CURRENT_USER\Control Panel\Desktop 下，新建项 MenuShowDelay(REG_SZ 类型，值设为 0)。

25. 删除多余的 DLL 文件

在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDlls 下，每个 DLL 文件的键值说明它已被几个应用程序所共享。如果是二进制“00 00 00 00”，则表明不被任何程序共享，可以删除。删除前先打开该键值，记下 DLL 文件的名称和位置，然后删除该键值和对应的文件。

26. 隐藏任务栏上“单击这里开始”的提示

在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 下，新建项 NoStartBanner(dword 类型)，键值为 1 表示隐藏该项提示；为 0 表示显示。

27. 记忆最后一次拨号上网用户的用户名和密码

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters 下，新建项 DisableSavePassword，REG_DWORD 类型，键值为 1 表示不记忆用户名和密码；为 0 则表示记忆。

28. 自动刷新窗口内容

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Update 下，查找 UpdateMode 项，默认键值为 1，表示手工刷新；改为 0，表示自动刷新。

29. 禁止将最近操作过的文档放入文档菜单历史记录中

在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 下，新建项 NoRecentDocsHistory(dword 类型)，键值为 1 表示禁止此项功能；为 0 表示允许此项功能。

30. 退出系统时，自动清除文档菜单中的历史记录

在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 下，新建项 ClearRecentDocsOnExit(dword 类型)，键值为 1 表示自动清除历史记录；为 0 表示不清除历史记录。

31. 应用程序出错时等待响应的时间(毫秒)

在 HKEY_CURRENT_USER\ControlPanel\desktop 下，查找项 HungAppTimeout 和 HungAppTimeout。它们的默认键值设为"5000 毫秒"，可以改为用户需要的值，来加快系统的响应速度和处理能力。

32. 关闭程序时的等待时间(毫秒)

运行"任务管理器/应用程序/结束任务"时，出现"结束任务"、"等待"提示时，选择"等待"的时间。在 HKEY_CURRENT_USER\ControlPanel\desktop 下，项为 WaitToKillApp-Timeout，默认键值为"5000 毫秒"，可减少该等待时间。

33. 自动关闭停止响应的程序

在 HKEY_CURRENT_USER\Control Panel\desktop 下，项 AutoEndTasks，键值为 1 表示自动关闭停止响应的程序；为 0 表示手工关闭。

34. 系统崩溃后自动重新启动

系统崩溃后会蓝屏、死机，开机重启动时会检查磁盘，很费时。可设置系统崩溃后自动可置为重新启动，方法是：

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl 下，将项 AutoReboot 的键值置为 1。

35. 清理安全日志

在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 下，项 crashonauditfail，键值为 1 表示自动处理安全日志；为 0 表示手工清理安全日志。

36. 激活 DOS 命令窗口快速编辑模式

在 HKEY_CURRENT_USER\Console 下，项 QuickEdit(dword 类型)，键值为 1 表示允许激活快速编辑模式；为 0 表示禁止激活快速编辑模式。

注意，对于不熟悉 Windows 内核及注册表内容的用户，修改注册表一定要谨慎，最好不要随意修改注册表，以免造成不必要的损失。另外，在修改注册表前，一定要先备份注册表，一旦修改后系统出错，可用备份的注册表恢复。

7.3.3 利用任务管理器进行进程管理

1. 如何启动任务管理器

在 Windows 2000/XP 下，按 Ctrl＋Alt＋Del 组合键，即进入“Windows 任务管理器”对话框，如图 7-8 所示。



图 7-8 “Windows 任务管理器”对话框

Windows 任务管理器共有应用程序、进程、性能、联网和用户等 5 个选项卡。

在任务管理器中选择“应用程序”选项卡即进入应用程序查看窗口，在该窗口下可以看到当前运行的所有应用程序，如图 7-8 所示。

2. 进程管理

在任务管理器中选择“进程”选项卡，即进入进程管理窗口，如图 7-9 所示。



图 7-9 任务管理器-进程管理

在图 7-9 所示的进程管理窗口中，可以看到当前在本机上运行的所有进程，以及进程用户、占用 CPU 时间(比率)、内存使用情况等信息。

可以根据图 7-9 所提供进程运行情况，可以发现可疑的进程以及运行异常(如 CPU 占用率过高、内存占用太大等)的进程，以便及时采取措施，比如对该进程进行监控，也可采取切断网络、关闭进程等措施。关闭进程的方法是在图 7-9 所示的进程管理窗口中，选择相应的进程，并单击“结束进程”按钮即可。

7.3.4 基于 Windows XP 环境的本地安全策略

1. 怎样进入本地安全策略

在 Windows XP 下单击“开始”|“控制面版”|“管理工具”|“本地安全策略”，即进入“本地安全设置”窗口，如图 7-10 所示。

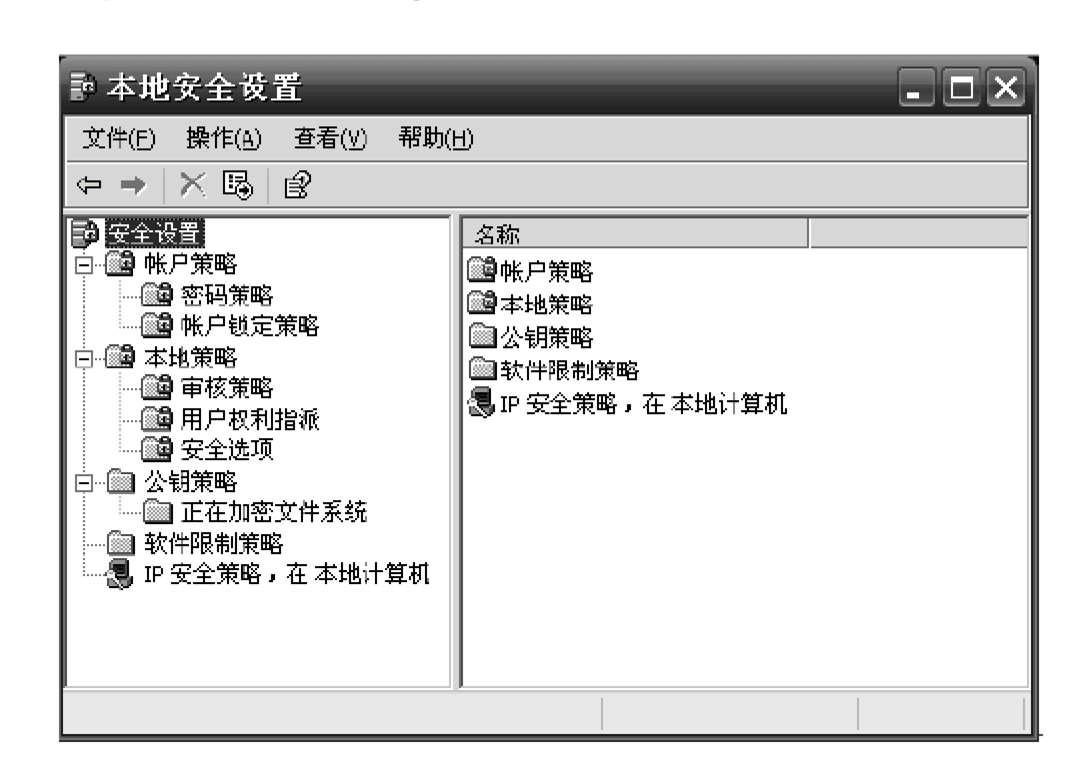


图 7-10 “本地安全设置”窗口

2. 本地安全策略的设置

从图 7-10 可看出，本地安全策略设置窗口一分为二，左边窗口是一个可展开的功能菜单，右边窗口是选中子项的安全策略内容。

在这里，以“密码策略”的设置为例，介绍基于 Windows XP 环境下本地安全策略的设置。

在图 7-10 所示的本地安全设置主窗口下，单击左窗口中的“账户策略”|“密码策略”子项，进入密码策略设置窗口，如图 7-11 所示。

如图 7-11 所示，密码策略有“密码复杂性、密码长度、密码最长存留期、密码最短存留期、强制历史密码和用户还原”等设置项。

1) 密码复杂性设置

密码复杂性设置用以确认密码是否要求符合复杂性要求。

在图 7-11 中，选择右窗口的“密码必须符合复杂性要求”设置项，右击，系统弹出一个下

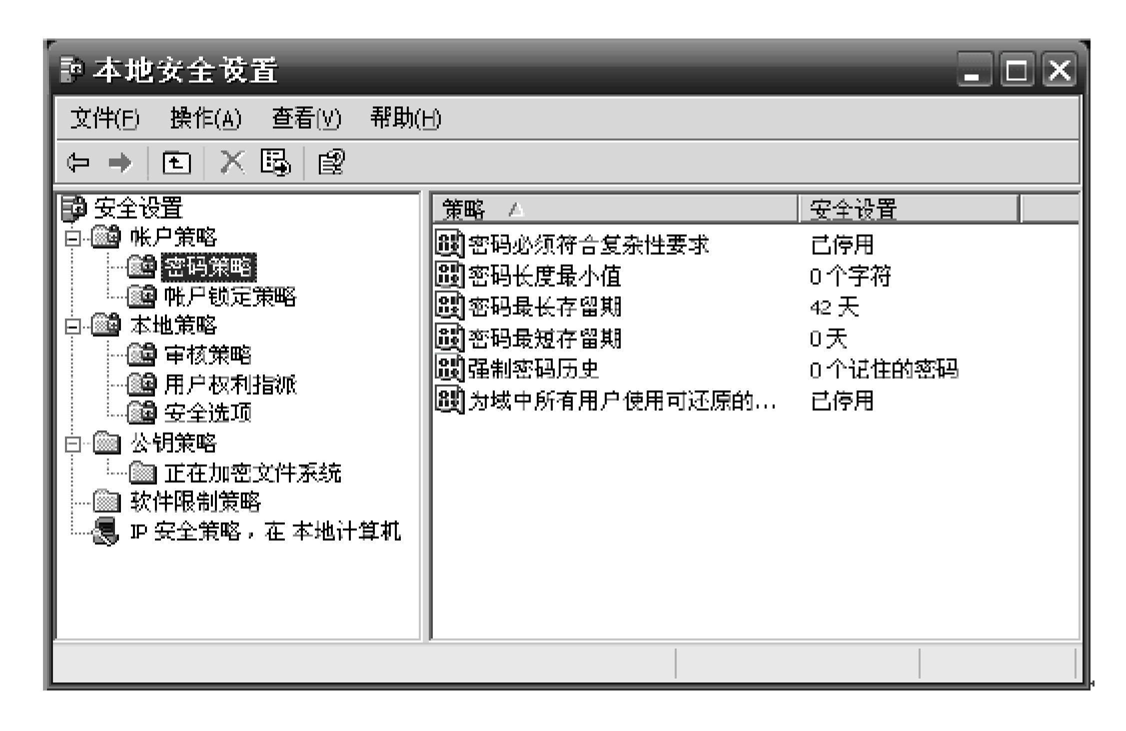


图 7-11　密码策略

拉式菜单，在该下拉菜单中选择“属性”命令，得到一个如图 7-12 所示的对话框。

根据要求选择“已启用”或“已禁用”选项并单击“确定”按钮。

2）密码长度的设置

密码长度设置用以指定密码的位数，根据现代密码学的要求，安全密码长度至少应在 6 位以上，最好是 8 位或 8 位以上。

在图 7-11 中，选择右窗口的“密码长度最小值”设置项，右击，系统弹出一个下拉式菜单，在该下拉菜单中选择“属性”命令，得到一个如图 7-13 所示的对话框。

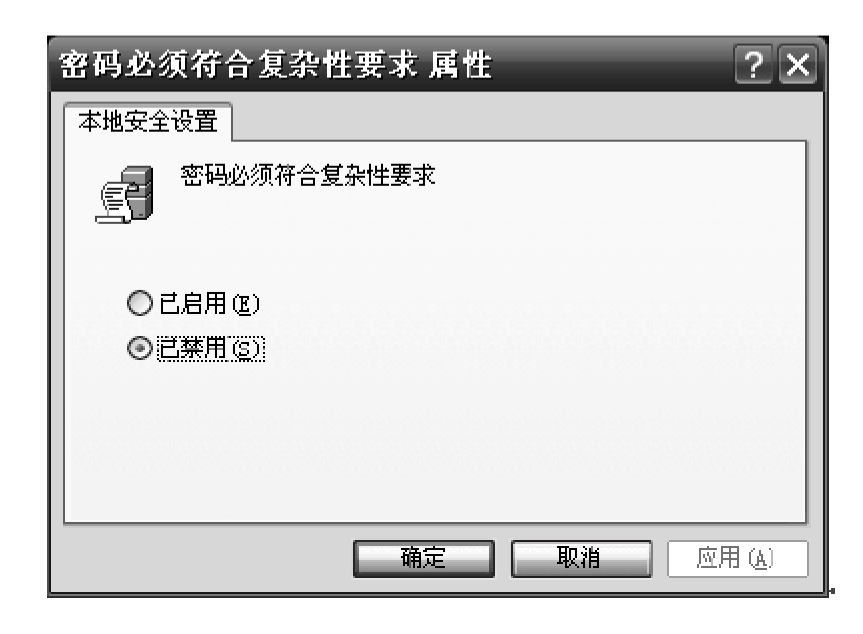


图 7-12　密码复杂性设置



图 7-13　密码长度设置

在图 7-13 中，选择一个密码长度后单击“确定”按钮，密码长度设置完毕。

其他安全策略设置方法与操作步骤与上述的密码设置方法与操作步骤相同。

习　题　7

1. Windows 2000 Server 的安全设置包括哪几个方面的内容？
2. Windows 2000 Server 的安全策略主要包括哪两大类？
3. Windows 2000 Server 安全策略的账户中保护安全策略的主要措施是什么？
4. Windows 2000 Server 安全策略的账户中系统监控安全策略的主要措施是什么？
5. UNIX 的安全体系结构的内容是什么？

第 8 章 chapter 8

防火墙技术

8.1 防火墙概述

8.1.1 防火墙的基本概念

1. 防火墙的基本概念

古时候，人们常在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。自然，这种墙因此而得名“防火墙(firewall)”。现在，如果一个网络连接了Internet，它的用户就可以访问外部世界并与之通信，同时，外部世界也同样可以访问该网络并与之交互。为安全起见，可以在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障，这道屏障的作用是阻断来自外部通过网络对本网络的威胁和入侵，提供扼守本地网络的安全和审计的关卡。这种中介系统叫做“防火墙”或“防火墙系统”。

防火墙是在两个网络间实现访问控制的一个或一组软硬件系统。防火墙的最主要功能就是屏蔽或允许指定的数据通信，而该功能的实现又主要是依靠一套访问控制策略，由访问控制策略来决定通信的合法性。

防火墙是在两个网络通信时执行的一种访问控制手段，它能允许“经同意”的人和数据进入用户的网络，同时将“未经同意”的人和数据拒之门外，最大限度地阻止网络中的非法用户来访问用户的网络，防止他们更改、复制和毁坏用户的重要信息。防火墙实质上就是一种过滤塞，只让经用户允许的内容通过这个塞子，别的内容都统统过滤掉。在网络的世界里，要由防火墙过滤的就是承载通信数据的通信包。

2. 防火墙的基本任务

防火墙在实施安全的过程中是至关重要的。一个防火墙策略要符合 4 个目标，而每个目标通常都不是通过一个单独的设备或软件来实现的。大多数情况下防火墙的组件放在一起使用以满足公司安全目的的需求。防火墙要能确保满足以下 4 个目标。

1）实现一个公司的安全策略

防火墙的主要意图是强制执行用户的安全策略。通过前面几章的学习认识到了网络安全中安全策略的重要性。关键的问题是如何通过防火墙来实施这些策略。

2）创建一个阻塞点

防火墙在一个公司私有网络和子网间建立一个检查点。这种实现要求所有的流量都要通过这个检查点。一旦这些检查点建立后，防火墙就可以监视、过滤和检查所有进来和出去的流量。网络安全产业称这些检查点为“阻塞点”。通过强制所有进出流量都通过这些检查点，网络管理员可以集中在一个地方来实现安全目的。如果没有这样一个供监视和控制信息的检查点，系统或安全管理员则要在很多地方来进行监测。检查点的另一个名字叫做“网络边界”。

3）记录 Internet 活动

防火墙还能够强制日志记录，并且提供警报功能。通过在防火墙上实现日志服务，安全管理员可以监视所有从外部网或互联网的访问。一个好的日志策略是实现适当网络安全的有效工具之一。防火墙对于管理员进行日志存档提供了更多的信息。

4）限制网络暴露

防火墙在用户的网络周围创建了一个保护的边界，并且对于公网隐藏了用户内部系统的一些信息以增加保密性。当远程结点试图侦测用户的网络时，他们仅仅能看到防火墙，远程设备将不会知道用户内部网络的布局以及存放的信息。防火墙利用提高认证功能和对网络加密来限制网络信息的暴露。通过对所有流量的检查，限制从外部发动的攻击。

3. 基本术语

1）网关(gateway)

网关是在两台设备之间提供转发服务的系统。网关的范围可以从互联网应用程序如公共网关接口(CGI)到在两台主机间处理流量的防火墙网关。这个术语是非常常见的，而且可用于一个防火墙组件里，在两个不同的网络路由间处理数据。

2）电路级网关(circuit level gateway)

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，这样来决定该会话是否合法，电路级网关是在 OSI 模型中会话层上来过滤数据包。另外，电路级网关还提供一个重要的安全功能，网络地址翻译(NAT)将所有公司内部的 IP 地址映射到一个“安全”的 IP 地址，这个地址是由防火墙使用的。有两种方法来实现这种类型的网关，一种是由一台主机充当筛选路由器而另一台充当应用级防火墙；另一种是在第一个防火墙主机和第二个防火墙主机之间建立安全的连接。

3）应用级网关(application level gateway)

应用级网关可以工作在 OSI 的 7 层模型的任一层上，能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做一些复杂的访问控制。

4）堡垒主机(bastion host)

堡垒主机应是在 Internet 高度暴露的，也是网络中最容易受到侵入的主机。堡垒主机也就是防火墙体系中的大无畏者，其目的是把敌人的火力吸引到自己身上，从而达到保护其他主机的目的。堡垒主机的设计思想就是检查点原则，把整个网络的安全问题集

中在某个主机上解决,从而省时省力,不用考虑其他主机的安全。通常情况下,堡垒主机上运行一些通用的网络操作系统,并存放一些不重要或已过期的机密文件。

5）双宿主机(dual homed host)

现代的防火墙系统大多是双宿主机,即有两个网络接口的计算机系统,其中一个接口连接内部网,另一个接口连接外部网。有的防火墙是多宿主机,有 3 个或多个网络接口,可以连接多个网络,实现多个网络之间的访问控制。

6）数据包过滤(package filter ring)

一些设备,如路由器、网关或双宿主机,可以有选择地控制网络上往来的数据流。当数据包要经过这些设备时,这些设备可以检查 IP 数据包的相应选项,根据既定的规则来决定是否允许数据包通过。

7）屏蔽路由器(screened router)

屏蔽路由器也叫过滤路由器,是一种可以根据过滤原则对数据包进行阻塞和转发的路由器,现在有很多路由器都具备包过滤的功能。

8）屏蔽主机(screened host)

被放置到屏蔽路由器后面网络上的主机称为屏蔽主机,该主机能被访问的程度取决于路由器的屏蔽规则。

屏蔽子网指位于屏蔽路由器后面的子网,子网能被访问的程度取决于屏蔽规则。

9）代理服务器(proxy server)

代理服务器就像中间人,是一种代表客户和服务器通信的程序,一般在应用层实现。典型的代理接受用户的请求,然后根据事先定义好的规则,决定用户或用户的 IP 地址是否有权使用代理服务器,然后代表客户建立一个与服务器之间的连接。

10）IP 地址欺骗(IP spoofing)

这是一种黑客的攻击形式,黑客使用一台机器上网,而借用另一台机器的 IP 地址,从而冒充另一台机器与服务器打交道。防火墙可以识别这种 IP 地址欺骗。

11）隧道路由器(tunneling router)

它是一种特殊的路由器,可以对数据包进行加密,让数据能通过非信任网,如 Internet,然后在另一端用同样的路由器进行解密。

12）虚拟专用网(Virtual Private Network,VPN)

一种连接两个远程局域网的方式,连接要通过非信任网,如 Internet,所以一般通过隧道路由器或 VPN 网关来实现互联。

13）DNS 欺骗(DNS spoofing)

通过破坏被攻击主机上的域名服务器的缓存,或破坏一个域名服务器来伪造 IP 地址和主机名的映射,从而冒充其他机器。DNS 欺骗现在也是黑客攻击服务器的常用手段。

14）Internet 控制报文协议(ICMP)

ICMP 的全称是 Internet Control Message Protocol(网间报文控制协议),它是 IP 不可分割的一部分,用来提供错误报告。一旦发现各种错误类型就将其返回原主机,最常见的 ping 命令就是基于 ICMP 的。ICMP 的统计信息包含收发的各种类型的 ICMP 报文的计数以及收发错误报文的计数。

15）纵深防御(defense in depth)

一种确保网络尽可能安全的安全措施，一般与防火墙联合使用。

16）最小特权(least privilege)

在运行和维护系统中，尽可能地减少用户的特权，但同时也要使用户有足够的权限来做事，这样就会减少特权被滥用的机会。内部人员滥用特权很可能在防火墙上打开一个安全缺口，这是很危险的，很多的入侵是由此引发的。

17）网络地址翻译(NAT)

网络地址解释是对 Internet 隐藏内部地址，防止内部地址公开。这一功能可以克服 IP 寻址方式的诸多限制，完善内部寻址模式。把未注册 IP 地址映射成合法地址，就可以对 Internet 进行访问。NAT 的另一个名字是 IP 地址隐藏。RFC1918 概述了地址并且 IANA 建议使用内部地址机制，以下地址作为保留地址。

10.0.0.0～10.255.255.255　　(A 类保留地址)

172.16.0.0～172.31.255.255　　(B 类保留地址)

192.168.0.0～192.168.255.255　(C 类保留地址)

如果用户选择上述列表中的网络地址，不需要向任何互联网授权机构注册即可使用。使用这些网络地址的一个好处就是在互联网上永远不会被路由。互联网上所有的路由器发现源或目标地址含有这些私有网络 ID 时都会自动丢弃。

18）非军事化区域(DMZ)

DMZ 是一个小型网络，存在于公司的内部网络和外部网络之间。这个网络由筛选路由器建立，有时是一个阻塞路由器。DMZ 用来作为一个额外的缓冲区以进一步隔离公网和用户的内部私有网络。DMZ 另一个名字叫做 Service Network，因为它非常方便。这种实施的缺点在于存在于 DMZ 区域的任何服务都不会得到防火墙的安全保护。

19）筛选路由器(sieve router)

筛选路由器的另一个术语就是包过滤路由器，它至少有一个接口是连向公网的，对进出内部网络的所有信息进行分析，并按照一定的安全策略——信息过滤规则对进出内部网络的信息进行限制，允许授权信息通过，拒绝非授权信息。信息过滤规则是以其所收到的数据包头信息为基础的。采用这种技术的防火墙优点在于速度快、实现方便，但安全性能差，且由于不同操作系统环境下 TCP 和 UDP 端口号所代表的应用服务协议类型有所不同，故兼容性差。

20）阻塞路由器

阻塞路由器也叫内部路由器，用以保护内部的网络，使之免受 Internet 和周边网的侵犯。阻塞路由器为用户的防火墙执行大部分的数据包过滤工作。它允许从内部网络到 Internet 的有选择的出站服务。内部路由器所允许的在堡垒主机和用户内部网之间服务可以不同于内部路由器所允许的在 Internet 和用户内部网之间的服务。限制堡垒主机和内部网之间服务的理由是减少由此而导致来自堡垒主机侵袭的机器的数量。

4. 防火墙的特性

大多数防火墙系统具有包过滤、电路级网关和应用级网关的功能。它们检查单独的数

据包或整个信息包,然后利用事先订制的规则来强制安全策略。只有那些可接受的数据包才能进出整个网络。当用户实施一个防火墙策略时,这 3 种防火墙类型可能都需要。更高级的防火墙提供额外的功能可以增强网络的安全性,每个防火墙都应该实施日志记录。

1) 认证

防火墙是一个合理的放置提供认证方法来避开特定的 IP 包。用户可以要求一个防火墙令牌(firewall token),或反向查询一个 IP 地址。反向查询可以检查用户是否真正地来自它所报告的源位置。这种技术有效地反击 IP 欺骗的攻击。防火墙还允许终端用户认证。应用级网关或代理服务器可以工作在 TCP/IP 的每一层上。多数的代理服务器提供完整的用户账号数据库。结合使用这些用户账号数据库和代理服务器自定义的选项来进行认证。代理服务器还可以利用这些账号数据库来提供更详细的日志。

2) 日志和警报

为了不降低网络性能和效率,在默认配置下,包过滤及筛选路由器是不进行日志记录的,更为重要的是,防火墙并不能对所有事件创建日志。筛选路由器只能记录一些最基本的信息,而电路级网关也只能记录少量的信息。因为用户要在防火墙上创建一个阻塞点,潜在的黑客必须要先穿过它。如果用户放置全面记录日志的设备并在防火墙本身实现这种技术,那么有可能捕获到所有用户的活动。可以确切地知道黑客在做什么并得到这些活动信息用于审计。一些防火墙允许用户预先配置对不期望的活动做出响应。防火墙两种最普通的活动是中断 TCP/IP 连接和自动发出警告。

8.1.2 防火墙的目的和作用

1. 构建网络防火墙的主要目的

- 控制访问者进入一个被严格控制的点。
- 防止进攻者接近防御设备。
- 控制内部人员从一个特别控制点离开。
- 检查、筛选、过滤和屏蔽信息流中的有害信息,防止对计算机和计算机网络进行恶意破坏。

防火墙的目的在于实现安全访问控制,在 OSI 体系结构中,防火墙可以在 OSI 中 7 层模型中的第 5 层设置。一般的防火墙模型如图 8-1 所示。

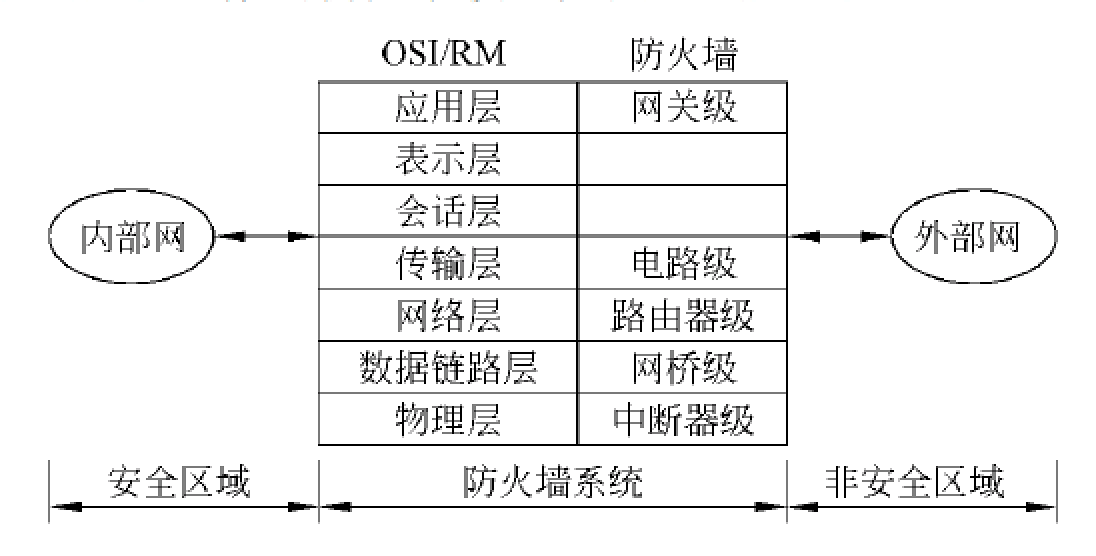


图 8-1 防火墙与 OSI 模型

2. 网络防火墙的主要作用

防火墙是一种非常有效的网络安全模型，通过它可以隔离内外网络，以达到网络中安全区域的连接，同时不妨碍人们对风险区域的访问。监控出入网络的信息，仅让安全的、符合规则的信息进入内部网络，为网络用户提供一个安全的网络环境。其主要作用如下：

- 有效收集和记录 Internet 上活动和网络误用情况。
- 能有效隔离网络中的多个网段，能有效地过滤、筛选和屏蔽一切有害的信息和服务。
- 防火墙就像一个能发现不良现象的警察，能执行和强化网络的安全策略。
- 保证对主机的安全访问。
- 保证多种客户机和服务器的安全性。
- 保护关键部门不受到来自内部的攻击和外部的攻击，为通过 Internet 与远程访问的雇员、客户、供应商提供安全通道。

3. 防火墙的特性

防火墙系统具有以下几方面的特性。

- 所有在内部网络和外部网络之间传输的数据都必须通过防火墙。
- 只有被授权的合法数据，即防火墙系统中安全策略允许的数据，可以通过防火墙。
- 防火墙本身可以经受住各种攻击。
- 使用目前新的信息安全技术。比如现代密码技术、一次口令系统及智能卡等。
- 人机界面友好、配置使用方便，易管理。系统管理员可以方便地对防火墙进行设置，对 Internet 的访问者、被访问者、访问协议以及访问方式进行控制。
- 广泛的服务支持。通过将动态的、应用层的过滤能力和认证相结合，可实现 WWW 浏览器、HTTP 服务器和 FTP 等。
- 对私有数据的加密支持。保证通过 Internet 进行虚拟私人网络和商务活动不受损坏。
- 客户端认证。只允许指定的用户访问内部网络或选择服务，是企业本地网与分支机构、商业伙伴和移动用户间安全通信的附加部分。
- 反欺骗。欺骗是从外部获取网络访问权的常用手段，防火墙能监视这样的数据包并能扔掉它们；C/S 模式和跨平台支持，能使运行在另一平台的管理模块控制运行在另一平台的监视模块。

8.1.3 防火墙的发展

1. 防火墙的发展历史

第 1 代防火墙技术几乎与路由器同时出现，采用了包过滤（packet filter）技术。1989 年，贝尔实验室的 Dave Presotto 和 Howard Trickey 推出了第 2 代防火墙，即电路层防

火墙，同时提出了第3代防火墙——应用层防火墙(代理防火墙)的初步结构。1992年，USC信息科学院的BobBraden开发出了基于动态包过滤(dynamic packet filter)技术的第4代防火墙，后来演变为目前所说的状态监视(stateful inspection)技术。1994年，以色列的CheckPoint公司开发出了第一个采用这种技术的商业化的产品。第5代防火墙是在1998年推出的，NAI公司推出了一种自适应代理(adaptive proxy)技术，并在其产品Gauntlet Firewall for NT中得以实现，给代理类型的防火墙赋予了全新的意义。高级应用代理(advanced application proxy)的研究，克服速度和安全性之间的矛盾，可以称之为第5代防火墙。

2. 防火墙的发展趋势

今后，防火墙将朝下列技术和方向发展：

动态包过滤；内核透明代理；用户强认证机制；加密技术；智能日志、审计跟踪和实时报警；内容和策略感知能力；内部信息隐藏技术；提高防火墙产品的集成性和采用分布式管理，加强防火墙之间的交互操作性。

8.2 防火墙的类型

8.2.1 包过滤防火墙

1. 包过滤型防火墙的基本功能

包过滤型防火墙(packet filter firewall)的包过滤器安装在路由器上，工作在网络层(IP)，因此也称为网络层防火墙。它基于单个包实施网络控制，根据所收到数据包的源地址、目的地址、源端口号及目的端口号、包出入接口、协议类型和数据包中的各种标志位等参数，与用户预定的访问控制表进行比较，判定数据是否符合预先制定的安全策略，决定数据包的转发或丢弃，即实施信息的过滤。它实际上是控制内部网络上的主机可直接访问外部网络，而外部网络上的主机对内部网络的访问则要受到限制。

这种防火墙的优点是简单、方便、速度快、透明性好，对网络性能影响不大，但它缺乏用户日志(log)和审计信息(audit)，缺乏用户认证机制，不具备登录和报告性能，不能进行审核管理，且过滤规则的完备性难以得到检验，过滤规则复杂难以管理，因此安全性较差。

2. 包过滤防火墙的优缺点

1) 优点

防火墙对每条传入和传出网络的包实行控制。

每个IP包的字段都被检查，例如源地址、目的地址、协议和端口等。防火墙将基于这些信息应用过滤规则。

防火墙可以识别和丢弃带欺骗性源IP地址的包。

包过滤防火墙是两个网络之间访问的唯一来源。因为所有的通信必须通过防火墙，

绕过是困难的。

包过滤通常被包含在路由器数据包中，所以不必额外的系统来处理这个特征。

2）缺点

配置困难。因为包过滤防火墙很复杂，人们经常会忽略建立一些必要的规则，或者错误配置了已有的规则，在防火墙上留下漏洞。然而，在市场上，许多新版本的防火墙对这个缺点正在作改进，如开发者实现了基于图形化用户界面(GUI)的配置和更直接的规则定义。

为特定服务开放的端口存在着危险，可能会被用于其他传输。例如，Web 服务器默认端口为 80，而计算机上又安装了 RealPlayer，那么它会搜寻可以允许连接到 RealAudio 服务器的端口，而不管这个端口是否被其他协议所使用，RealPlayer 正好是使用 80 端口而搜寻的。就这样，RealPlayer 无意中利用了 Web 服务器的端口。

“包过滤”技术是用关键词进行“包内容”的检查和过滤的，因此，对于“图片”信息，防火墙是不能对其内容进行“过滤”检查的。

攻击者绕过防火墙进入网络，例如拨号连接。换句话说，防火墙是不能阻止对于“绕道而行”进入网络的攻击的。

8.2.2 代理服务器

1. 代理服务器防火墙的基本功能

代理服务器防火墙(proxy service firewall)通过在主机上运行代理服务程序，直接对特定的应用层进行服务，因此也称为应用层防火墙。其核心是运用防火墙主机上的代理服务器进程，代理网络用户完成 TCP/IP 功能，实际上是为特定网络应用而连接两个网络的网关，且对不同的应用(如 E-mail、FTP、Telnet 和 WWW 等)都应用一个不同的代理。代理服务可以实施用户认证、详细日志、审计跟踪、数据加密等功能和对具体协议及应用的过滤，如阻止 Java 或 Java Script 程序的运行。

应用程序代理防火墙实际上并不允许在它连接的网络之间直接通信。它只接受来自内部网络特定用户应用程序的通信，然后建立于公共网络服务器单独的连接。网络内部的用户不直接与外部的服务器通信，所以服务器不能直接访问内部网的任何一部分。

另外，如果不为特定的应用程序安装代理程序代码，这种服务是不会被支持的，不能建立任何连接。这种建立方式拒绝任何没有明确配置的连接，从而提供了额外的安全性和控制性。

应用程序代理防火墙可以配置成允许来自内部网络的任何连接，它也可以配置成要求用户认证后才建立连接。要求认证的方式由只为已知的用户建立连接的这种限制，为安全性提供了额外的保证。如果网络受到危害，这个特征使得从内部发动攻击的可能性大大减少。

2. 代理防火墙的优缺点

1）优点

指定对连接的控制，例如允许或拒绝基于服务器 IP 地址的访问，允许或拒绝基于用

户所请求连接的 IP 地址的访问。

通过限制某些协议的传输请求，以减少网络中不必要的服务。

大多数代理防火墙能够记录所有的连接，包括地址和持续时间。这些信息对追踪攻击和发生的未授权访问的事件是很有用的。

2）缺点

必须在一定范围内定制用户系统，这取决于所用的应用程序。

一些应用程序不支持代理连接。

8.2.3 电路层网关

电路层网关(circuit gateway)在网络的传输层上实施访问策略，是在内、外网络主机之间建立一个虚拟电路进行通信，相当于在防火墙上直接开了个口子进行传输，不像应用层防火墙那样能严密控制应用层的信息。

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，这样来决定该会话(session) 是否合法，电路级网关是在 OSI 模型中会话层上来过滤数据包的。

实际上，电路级网关并非作为一个独立的产品存在，它通常与其他的应用级网关结合在一起，如 TrustInformationSystems 公司的 GauntletInternetFirewall；DEC 公司的 AltaVistaFirewall 等产品。另外，电路级网关还提供一个重要的安全功能，代理服务器(proxy server)，代理服务器是在其上运行一个叫做“地址转移”的进程，将所有内部 IP 地址映射到一个外部 IP 地址，这个地址是由防火墙使用的。但是，作为电路级网关也存在着一些缺陷，因为该网关是在会话层工作的，无法检查应用层级的数据包。

8.2.4 混合型防火墙

混合型防火墙(hybrid firewall)是把过滤和代理服务等功能结合起来，形成新的防火墙，所用主机称为堡垒主机，负责代理服务。

混合型防火墙采用的技术如下：

- 动态包过滤。
- 内核透明技术。
- 用户认证机制。
- 内容和策略感知能力。
- 内部信息隐藏。
- 智能日志、审计和实时报警。
- 防火墙的交互操作性。
- 各种安全技术的有机结合等。

8.2.5 应用级网关

应用级网关(application gateway)使用专用软件来转发和过滤特定的应用服务，如

Telnet、FTP 等服务连接。

应用级网关能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做一些复杂的访问控制。但每一种协议需要相应的代理软件，使用时工作量大，效率不如网络级防火墙。

常用的应用级防火墙已有了相应的代理服务，例如 HTTP、NNTP、FTP、Telnet、Rlogin 和 X-Window 等，但是，对于新开发的应用，尚没有相应的代理服务，它们将通过网络级防火墙和一般的代理服务。

应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏"透明度"。在实际使用中，用户在受信任的网络上通过防火墙访问 Internet 时，经常会发现存在延迟并且必须进行多次登录(login)才能访问 Internet 或 Intranet。

8.2.6 状态/动态检测防火墙

1. 状态/动态检测防火墙的基本功能

状态/动态检测防火墙，试图跟踪通过防火墙的网络连接和包，这样防火墙就可以使用一组附加的标准，以确定是否允许或拒绝通信。这一目标是在使用了基本包过滤防火墙的通信上应用一些技术实现的。

包过滤防火墙对一个数据包是允许还是拒绝，完全取决于包自身所包含的内容，如源地址、目的地址和端口号等。如果数据包中没有包含任何描述它在信息流中的位置的信息，则认为该包是无状态的，一个状态包检查防火墙跟踪的包中必须包含所需的信息。

一个状态/动态检测防火墙可截断所有传入的通信，而允许所有传出的通信。只有按要求传入的数据被允许通过，直到连接被关闭为止，而未被请求的传入通信被截断。

状态/动态检测防火墙可提供的额外服务如下：

- 将某些类型的连接重定向到审核服务中去。例如，专用 Web 服务器的连接，在 Web 服务器连接被允许之前，可能被发到 SecutID 服务器(用一次性口令来使用)。
- 拒绝携带某些数据的网络通信，如带有附加可执行程序的传入电子消息，或包含 ActiveX 程序的 Web 页面。

跟踪连接状态的方式取决于包通过防火墙的类型。

- TCP 包。当建立起一个 TCP 连接时，通过的第一个包被标有包的 SYN 标志。通常情况下，防火墙丢弃所有外部的连接企图，除非已经建立起某条特定规则来处理。
- UDP 包。UDP 包比 TCP 包简单，因为它们不包含任何连接或序列信息。它们只包含源地址、目的地址、校验码和携带的数据。这种信息的缺乏使得防火墙确定包的合法性很困难，因为没有打开的连接可利用，以测试传入的包是否应被允许通过。对传入的包，若它所使用的地址和 UDP 包携带的协议与传出的连接请

求匹配，该包就被允许通过。防火墙能跟踪传出的请求，并详细记录下所使用的地址、协议和包的类型，然后对照保存过的信息核对传入的包，以确保这些包是被请求的。

2. 状态/动态检测防火墙的优缺点

1）优点

- 具有检查 IP 包的每个字段的能力，并遵从基于包中信息的过滤规则。
- 具有识别带有欺骗性源 IP 地址包的能力。
- 包过滤防火墙是两个网络之间访问的唯一来源。因为所有的通信必须通过防火墙，绕过是困难的。
- 基于应用程序信息验证一个包的状态的能力，例如基于一个已经建立的 FTP 连接，允许返回的 FTP 包通过。
- 基于应用程序信息验证一个包状态的能力，例如允许一个先前认证过的连接继续与被授予的服务通信。
- 记录有关通过的每个包的详细信息的能力。基本上，防火墙用来确定包状态的所有信息都可以被记录，包括应用程序对包的请求，连接的持续时间，内部和外部系统所做的连接请求等。

2）缺点

状态/动态检测防火墙唯一的缺点就是所有这些记录、测试和分析工作可能会造成网络连接的某种迟滞，特别是在同时有许多连接激活的时候，或者是有大量的过滤网络通信的规则存在时。特别是，硬件速度越快，这个问题就越不易察觉，而且防火墙的制造商一直致力于提高他们产品的速度。

8.2.7 网络地址翻译

1. NAT 的基本功能

网络地址翻译（Netware Address Translation，NAT）协议是将内部网络的多个 IP 地址转换到一个公共 IP 地址与 Internet 连接。

当内部用户与一个公共主机通信时，NAT 能追踪是哪一个用户所发出的请求，修改传出的包，这样包就像是来自单一的公共 IP 地址，然后再打开连接。一旦建立了连接，在内部计算机和 Web 站点之间来回流动的通信就都是透明的。

当从公共网络传来一个未经请求的连接时，NAT 有一套规则来决定如何处理它。如果没有事先定义好的规则，NAT 可丢弃所有未经请求的传入连接，就像包过滤防火墙所做的那样。

2. 地址翻译技术

1）静态翻译

一个指定的内部主机有一个固定不变的地址翻译表，通过这张表，可将内部地址翻

译成防火墙的外网接口地址。

2）动态翻译

为了隐藏内部主机的身份或扩展内部网络的地址空间，一个大的 Internet 客户群共享一组较小的 Internet IP 地址。

3）负载平衡翻译

一个 IP 地址和端口被翻译为同等配置的多个服务器，当请求到达时，防火墙将按照一个算法来平衡所有连接到内部的服务器，这样向一个合法 IP 地址请求，实际上是有多台服务器在提供服务。

4）网络冗余翻译

多个 Internet 连接被附加在一个 NAT 防火墙上，而这个防火墙根据负载和可用性对这些连接进行选择和使用。

3. NAT 的优缺点

1）优点

所有内部的 IP 地址对外面的人来说是隐蔽的。因为这个原因，网络之外没有人可以通过指定 IP 地址的方式直接对网络内的任何一台特定的计算机发起攻击。

如果因为某种原因公共 IP 地址资源比较短缺的话，NAT 可以使整个内部网络共享一个 IP 地址。

可以启用基本的包过滤防火墙安全机制，因为所有传入的包如果没有专门指定配置到 NAT，那么就会被丢弃。内部网络的计算机就不可能直接访问外部网络。

2）缺点

NAT 的缺点和包过滤防火墙的缺点是一样的。虽然可以保障内部网络的安全，但它也有一定的局限性。而且内网可以利用流传较广的木马程序，可以通过 NAT 做外部连接，就像穿过包过滤防火墙一样容易。

8.2.8 个人防火墙

1. 个人防火墙的基本功能

个人防火墙是一种能够保护个人计算机系统的安全软件，它可以直接在用户的计算机上运行，使用与状态/动态检测防火墙相同的方式来保护计算机免受攻击。个人防火墙是安装在计算机网络接口的较低级别上，用以监视传入传出网卡的所有网络通信。

一旦安装上个人防火墙，就可以把它设置成“学习模式”，这样的话，对遇到的每一种新的网络通信，个人防火墙都会提示用户一次，询问如何处理这种通信。然后个人防火墙便记住响应方式，并应用于以后遇到的相同网络通信。

例如，如果用户已经安装了一台个人 Web 服务器，个人防火墙可能将第一个传入的 Web 连接作上标志，并询问用户是否允许它通过。用户可能允许所有的 Web 连接、来自某些特定 IP 地址范围的连接等，个人防火墙然后把这条规则应用于所有传入的 Web 连接。

2. 个人防火墙的优缺点

1）优点

增加了保护级别，不需要额外的硬件资源。个人防火墙除了可以抵挡外来攻击的同时，还可以抵挡内部的攻击。

2）缺点

个人防火墙主要的缺点就是对公共网络只有一个物理接口。真正的防火墙应当监视并控制两个或更多的网络接口之间的通信。这样一来，个人防火墙本身容易受到威胁，或者说是具有这样一个弱点，网络通信可以绕过防火墙的规则进行。

8.29 智能防火墙

智能防火墙从技术特征上看，是利用统计、记忆、概率和决策的智能方法来对数据进行识别，并达到访问控制的目的。

一个典型的例子可以说明智能防火墙对网络安全是很重要的。传统的防火墙对包的检查，就像对人的相貌的识别，采用图像识别一样。把一个人的相貌转换为图像，对图像的每一个像素进行记忆，然后进行匹配检查。通过检查上千万个像素之后，告诉你，这是谁，这就是智能识别。智能防火墙无须海量计算就可以轻松找到网络行为的特征值来识别网络行为，从而轻松的执行访问控制。

1. 智能防火墙的关键技术

1）防攻击技术

智能防火墙能智能识别恶意数据流量，并有效地阻断恶意数据攻击。智能防火墙可以有效地解决 SYN Flooding、Land Attack、UDP Flooding、Fraggle Attack、Ping Flooding、Smurf、Ping of Death 及 Unreachable Host 等攻击。防攻击技术还可以有效的切断恶意病毒或木马的流量攻击。

2）防扫描技术

智能防火墙能智能识别黑客的恶意扫描，并有效地阻断或欺骗恶意扫描者。对目前已知的扫描工具如 ISS、SSS 和 NMAP 等扫描工具，智能防火墙可以防止被扫描。防扫描技术还可以有效地解决代表或恶意代码的恶意扫描攻击。

3）防欺骗技术

智能防火墙提供基于 MAC 的访问控制机制，可以防止 MAC 欺骗和 IP 欺骗，支持 MAC 过滤，支持 IP 过滤。将防火墙的访问控制扩展到 OSI 的第 2 层。

4）入侵防御技术

智能防火墙为了解决准许放行包的安全性，对准许放行的数据进行入侵检测，并提供入侵防御保护。入侵防御技术采用了多种检测技术，特征检测可以准确检测已知的攻击，特征库涵盖了目前流行的网络攻击；异常检测基于对监控网络的自学习能力，可以有效地检测新出现的攻击；检测引擎中还集成了针对缓冲区溢出等特定攻击的检测。智能防火墙完成了深层数据包监控，并能阻断应用层攻击。

5）包擦洗和协议正常化技术

智能防火墙支持包擦洗技术，对 IP、TCP、UDP 和 ICMP 等协议的擦洗，实现协议的正常化，消除潜在的协议风险和攻击。这些方法对消除 TCP/IP 协议的缺陷和应用协议的漏洞所带来的威胁，效果显著。

2. 智能防火墙的功能和特点

智能防火墙成功地解决了普遍存在的拒绝服务攻击的问题、病毒传播的问题和高级应用入侵的行为，代表着防火墙的主流发展方向。新一代的智能防火墙自身的安全性较传统的防火墙有很大的提高，在特权最小化、系统最小化、内核安全、系统加固、系统优化和网络性能最大化方面，与传统防火墙相比，有质的飞跃。

智能防火墙执行全访问的访问控制策略，而不是简单的过滤。基于对行为的识别，可以根据什么人、什么时间、什么地点、什么行为来执行访问控制，大大增强了防火墙的安全性，使其更加聪明和智能。

智能防火墙具备集中网络管理平台，具备配置管理、性能管理、故障管理、安全管理和审计管理 5 大管理域。

智能防火墙提供网络实时监控功能。支持监控防火墙的性能，如 CPU、内存、网络和硬盘的使用率等信息。支持监控防火墙的状态，并实时报警。支持实时监控，包括性能监控、接口流量监控等。

智能防火墙提供对日志的监控、自动处理、人工或自动导出、数据库导入、查看、查询、显示和报警等功能，并支持条件查询。

3. 智能防火墙的典型应用

除传统防火墙的应用外，智能防火墙还有以下特殊应用场合。

保护网络和站点免受黑客的攻击。由于目前众多的防火墙无法抵御 DDoS 的攻击，使得网站和网络频繁遭受黑客的攻击。采用智能防火墙，可以有效解决 DDoS 攻击。

阻断病毒的恶意传播。智能防火墙可以智能识别病毒的恶意扫描和流量攻击，有效切断恶意病毒的传播途径。由于智能防火墙是从流量异常来判断病毒的传播，避免了每一次新病毒的爆发所带来的灾难。

有效监控和管理内部局域网。传统的防火墙只防外不防内，导致内部局域网速度慢，恶意病毒和木马盛行。智能防火墙的防欺骗功能和 MAC 控制功能，能有效发现内部恶意流量，帮助安全管理员来找到攻击源。

保护必需的应用安全。智能防火墙的入侵防护功能，深层的应用数据检测可以有效的发现对应用的恶意攻击，并加以制止。

提供强大的身份认证授权和审计管理。对优化进行身份鉴别授权和审计，是网络安全的要素之一，基于人而不是 IP 进行管理，更能有效的进行网络安全管理，也为网络取证提供防抵赖的功能。

8.3 防火墙的设计与实现

8.3.1 防火墙的设计技术

为了网络的安全可靠，防火墙必须满足以下设计要求。

- 防火墙应由多个构件组成，形成一个有一定冗余度的安全系统，避免成为网络的单失效点。
- 防火墙应能抵抗网络黑客的攻击，并可对网络通信进行监控和审计。
- 防火墙一旦失效、系统重启或系统崩溃时，则应完全阻断内、外网络站点的连接，以防非法用户闯入。
- 防火墙应提供强制认证服务，外部网络站点对内部网络的访问应经过防火墙的认证检查，包括对网络用户和数据源的认证。应支持 E-mail、FTP、Telnet 和 WWW 等服务。
- 防火墙对内部网络应做到屏蔽作用，并且隐藏内部网站的地址和内部网络的拓扑结构。

在防火墙设计中，安全策略是防火墙的灵魂和基础。通常，防火墙采用的安全策略有如下两个基本准则。

- 一切未被允许的访问就是禁止的。
- 一切未被禁止的访问就是允许的。

建立防火墙是在对网络的服务功能和拓扑结构仔细分析的基础上，在被保护的网络周边，通过专用硬件、软件及管理措施的综合，对跨越网络边境的信息，提供监测、控制甚至修改的措施。

8.3.2 防火墙的实现技术

1）决定防火墙的类型与拓扑结构

针对防火墙所保护的系统安全级别作出定性和定量评估，从系统的成本、安全保护实现的难易程度以及升级、改造和维护的难易程度，决定该防火墙的类型和拓扑结构。

2）制定安全策略

在实现过程中，没有被允许的服务是被禁止的，没有被禁止的服务都是允许的。网络安全的第一策略是拒绝一切未许可的服务，即由防火墙逐项删除未许可的服务后，再转发信息。在此策略的指导下，再针对系统制定各项具体策略。

3）确定包过滤规则

一般以处理 IP 数据包包头信息为基础，包括过滤规则、过滤方式、源和目的端口号及协议类型等，它决定算法执行时顺序，因此正确的排列顺序至关重要。

4）防火墙维护和管理方案的制定

防火墙的日常维护是对访问记录进行审计，发现入侵和非法访问，据此对防火墙的安全性进行评价，需要时进行适当改进。管理工作要根据拓扑结构的改变或安全策略的变化，对防火墙进行硬件与软件的修改和升级。通过维护和管理进一步优化其性能，以保证网络及其信息的安全性。

8.4 防火墙安全管理技术

8.4.1 防火墙的安全性

防火墙是网络上使用最多且最重要的安全设备，是网络安全的重要基石。但防火墙不是万能的，有一定的缺陷和局限性。正确认识和使用防火墙，确保网络的安全使用，研究防火墙的局限性和脆弱性是十分必要的。

1. 防火墙的脆弱性

- 防火墙的操作系统不能保证没有漏洞。
- 防火墙的硬件不能保证不失效。所有的硬件都有一个生命周期，都会老化，总有失效的一天。
- 防火墙软件不能保证没有漏洞。防火墙软件也是软件，是软件就会有漏洞。
- 防火墙无法解决 TCP/IP 等协议的漏洞。防火墙本身就是基于 TCP/IP 等协议来实现的，无法解决 TCP/IP 本身具有的漏洞。
- 防火墙无法区分恶意命令还是善意命令。有很多命令对管理员而言，是一项合法命令，而在黑客手里就可能是一个危险的命令。
- 防火墙无法区分恶意流量和善意流量。一个用户使用 ping 命令，可用作网络诊断，也可用作网络攻击，在流量上是没有差异的。
- 防火墙的安全性与多功能成反比。多功能与防火墙的安全原则是背道而驰的。因此，除非确信需要某些功能，否则，应将功能最小化。
- 防火墙的安全性和速度成反比。防火墙的安全性是建立在对数据的检查之上，检查越细越安全，但检查越细速度越慢。
- 防火墙的多功能与速度成反比。防火墙的功能越多，对 CPU 和内存的消耗越大，功能越多，检查的越多，速度越慢。
- 防火墙无法保证准许服务的安全性。防火墙准许某项服务，却不能保证该服务的安全性。准许服务的安全性问题必须由应用安全来解决。
- 限制有用的网络服务。防火墙为了提高被保护网络的安全性，限制或关闭了很多有用但存在安全缺陷的网络服务。
- 无法防护内部网络用户的攻击。目前防火墙只提供对外部网络用户攻击的防护，对来自内部网络用户的攻击只能依靠内部网络主机系统的安全性（智能防火墙例外）。
- Internet 防火墙无法防范通过防火墙以外的其他途径的攻击。例如，在一个被保

护的网络上没有限制的拨号登录，内部网络上的用户就可以直接通过 SLIP 或 PPP 连接进入 Internet。

- Internet 防火墙不能完全防止传送已感染病毒的软件或文件。
- 不能防范新的网络安全威胁。防火墙是一种被动式的防护手段，它只能对已知的网络威胁起防护作用。

2. 防火墙的局限性

- 防火墙不能防范不经过防火墙的攻击。没有经过防火墙的数据，防火墙无法检查。
- 防火墙不能防止策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备，就像门卫一样，要根据政策规定来执行安全检查，而不能自作主张。
- 防火墙不能防止可接触的人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在于一个安全的地方。
- 防火墙不能防止利用网络协议中的缺陷进行的攻击。
- 防火墙不能防止利用服务器系统漏洞所进行的攻击。黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击，防火墙不能防止。
- 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时，会导致数据驱动式的攻击。
- 防火墙不能防止内部的泄密行为。防火墙内部的一个合法用户主动泄密，防火墙是无能为力的。
- 防火墙不能防止本身的安全漏洞的威胁。防火墙保护别人有时却无法保护自己，目前还没有厂商绝对保证防火墙不会存在安全漏洞。因此对防火墙也必须提供某种安全保护。

8.4.2 防火墙的安全策略

1. 用户账号策略

用户账号应包含用户的所有信息。其中最主要的应包括用户名、口令、用户所属的工作组、用户在系统中的权限和资源访问许可。

2. 用户权限策略

用户权限策略用来允许授权用户使用系统资源。用户权限一般有两类，第一类是对执行特定任务用户的授权可应用于整个系统；第二类是对特定对象（如目录、文件和打印机等）的规定，这些规定限制用户能否或以何种方式存取对象。其中第一类的权限要高于第二类。通常授予用户的权限有以下几种：

- 通过网络连接计算机。
- 备份文件和目录，此权限要高于文件和目录许可。

- 设置计算机内部系统时钟。
- 从计算机键盘登录计算机。
- 指定何种事件和资源被审查，查看和清除安全日志。
- 恢复文件和目录。
- 关闭系统。
- 获取一台计算机的文件、目录或是其他对象的所有权。

3. 信任关系策略

通过信任关系在网络中建立域模型的安全性。信任关系是在两个域中，一个域信任另外的域，它包括两个方面，信任域和被信任域。信任域可允许被信任域中的用户在其中使用。两个域信任关系的建立可以允许一个域中建立的用户存取整个网络中的资源。

1）单向信任

单向信任只是一个域信任另外一个域，如图8-2所示。典型的应用就是远程访问，它们之间并不相互信任，远程用户只可以在被信任域中使用。

2）双向信任

双向信任是两个域对等的互相信任，如图8-3所示，远程用户可以使用双方授权的资源。双向连接的信任关系只不过是两个单向信任关系，每个域都信任另外一个。



图8-2 单向信任关系　　图8-3 双向信任关系

3）多信任

更复杂的是在域间可以建立多个信任关系，如图8-4所示。几个域信任一个域来保证用户的统一管理，或是一个域信任几个域来保证用户延伸到多个域中，同时还可提供传递验证功能。

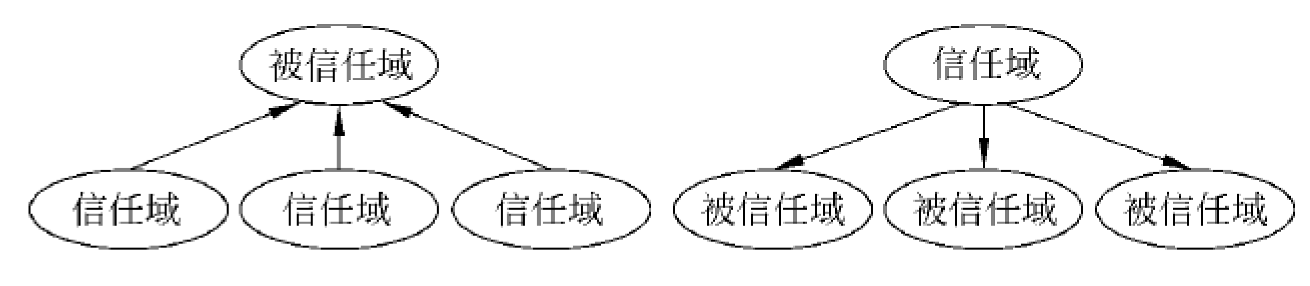


图8-4 多重信任关系

4. 包过滤策略

根据过滤规则，来过滤基于标准的数据包，完成包过滤功能。包过滤策略如下：

- 包过滤控制点。
- 包过滤操作过程。
- 包过滤原则。
- 防止两类不安全设计的措施。
- 对特定协议包的过滤。

5. 认证、签名和数据加密策略

目前可以公开的加密算法很多,其中最著名的传统加密算法是 DEC、RC4、RC5、RC6 以及现在准备替代 DES 的 AES 候选算法。最著名的公开密钥体制是 RSA 体制和 ELGamal 体制等。最有名的数字签名体制是 RSA 体制、DSS 体制、ELGamal 体制和椭圆曲线体制等。最有名的消息认证体制是 MD5 和 SHA-1 等。

因此在加密算法的选取应从两个方面入手,一方面从这些算法中选取 3DES、RC4、IDEA、RSA 和 MD5 等算法作为系统的核心加密算法,保证系统符合国际标准;另一方面根据我国的商业密码管理条例,在国内的重要部门使用保密通信系统中,必须使用国内认可的密码算法。

6. 密钥管理策略

Internet 的加密算法有两个困难。首先,通信双方之间的通信可能会通过多个网络,这些网络通常具有不同的安全机制,有的甚至根本不提供安全机制,这就使通信双方之间建立密钥的过程更加容易受到攻击。其次,不同网络的密钥管理协议可能不尽相同,这就导致用同样的协议来建立异网通信密钥和内部通信密钥会非常困难,增加了密钥管理机制的复杂性,很难实现密钥使用上的方便性。

从 Internet 应用来看,密钥管理方式应采用自动化管理,特别是对于密钥分配而言,应采用离线式密钥中心方式。针对 Internet 的层次结构,密钥中心的设置应具有相适应的层次。现代密钥体系也应采用层次结构,以分为主密钥、密钥加密密钥和会话密钥三个层次为宜。在密钥体制采用上,将采用对称密钥密码体制和公开密钥密码体制相结合的方法,以提高密钥分配的效率。

7. 审计策略

审计用来记录如下事件。

- 哪一个用户访问哪一个对象。
- 访问类型。
- 访问过程是否成功。
- 所有事件的审查都保存在安全日志中,安全日志记录通过的包和被滤掉的包的有关信息。

8.4.3 防火墙安全技术

前面介绍了防火墙的基本概念、体系结构等,本小节介绍防火墙的安全技术,包括数据包过滤技术、代理技术、状态检查技术和地址翻译技术(NAT)等。

1. 数据包过滤技术

1) 数据包过滤技术的基本原理

数据包过滤技术是防火墙最常用的技术。对于一个充满危险的网络,过滤路由器提

供了一种方法,用这种方法可以阻塞某些主机和网络连入内部网络,也可以用它来限制内部人员对一些危险和色情站点的访问。

顾名思义,数据包过滤技术是在网络中适当的位置对所有数据包实施过滤或筛选,只有满足过滤规则的数据包才被转发至相应的网络接口,其余数据包则从数据流中删除。

数据包过滤可以控制站点与站点、站点与网络、网络与网络之间的相互访问,但不能控制传输的数据内容,因为数据内容是应用层数据,不是包过滤系统所能辨认的,数据包过滤允许在某个地方为整个网络提供特别的保护。

包过滤检查模块深入到系统的网络层和数据链路层之间。因为数据链路层是事实上的网卡(NIC),网络层是第1层协议堆栈,所以防火墙位于软件层次的最底层。

包过滤一般要检查下面几项。

- IP 源地址。
- IP 目标地址。
- 协议类型(TCP 包、UDP 包和 ICMP 包)。
- TCP 或 UDP 的源端口。
- TCP 或 UDP 的目标端口。
- ICMP 消息类型。
- TCP 报头中的 ACK 位。

包过滤在本地端接收数据包时,一般不保留上下文,只根据目前数据包的内容做决定。根据不同的防火墙类型,包过滤可能在进入或输出防火墙时进行。可以拟定一个要接受的设备和服务的清单,一个不接受的设备和服务的清单,组成访问控制表。

2) 配置步骤

- 必须知道什么样的包允许通过,什么样的包不允许通过。
- 必须正式规定允许的包类型、包字段的逻辑表达。
- 必须用防火墙支持的语法重写表达式。

3) 按地址过滤规则实例

例 8-1 该实例是一个最简单的数据包过滤方式,它按照源地址进行过滤。若认为网络 210.40.8.0 是一个危险的网络,那么就可以用源地址过滤禁止内部主机和该网络进行通信。表 8-1 是根据这种策略所制定的规则。

表 8-1 包过滤规则表

规 则	方 向	源 地 址	目 标 地 址	动 作
A	出	内部网络	210.40.8.0	拒绝
B	入	210.40.8.0	内部网络	拒绝

4) 按服务过滤规则实例

例 8-2 设安全策略是禁止外部主机访问内部的 E-mail 服务器(SMTP,端口 25),允许内部主机访问外部主机,实现这种的过滤的访问控制规则如表 8-2 所示。

表 8-2 服务过滤规则表

规　则	方　向	动　作	源地址	源端口	目的地址	目的端口	注　　释
A	进	拒绝	M	*	E-mail	25	不信任
B	出	允许	*	*	*	*	允许连接
C	双向	拒绝	*	*	*	*	默认状态

规则按从前到后的顺序匹配，字段中的"*"代表任意值，没有被过滤器规则明确允许的包将被拒绝。就是说，每一条规则集都跟随一条含蓄的规则，就像表 8-2 中的规则 C。这与一般原则是一致的，没有明确"允许"的就是被"禁止"的。

任何一种协议都是建立在双方的基础上的，信息流也是双向的。规则总是成对出现的。

5）包过滤实例

例 8-3 第一，假设一个类网络 116.111.4.0，发现站点 202.208.5.6 上有黄色的 BBS，所以希望阻止网络中的所有用户访问该点的 BBS；再假设这个站点的 BBS 服务是通过 Telnet 方式提供的，那么需要阻止到那个站点的出站 Telnet 服务，对于 Internet 的其他站点，允许内部的网用户通过 Telnet 方式访问，但不允许其他站点以 Telnet 方式访问网络。第二，为了收发电子邮件，允许 SMTP 出站入站服务，邮件服务器是 IP 地址为 116.111.4.1。第三，对于 WWW 服务，允许内部网用户访问 Internet 上任何网络和站点，但只允许一个公司的网络访问内部 WWW 服务器，内部 WWW 服务器的 IP 地址为 116.111.4.5，因为是合作伙伴关系，并设合作伙伴网络为 98.120.8.0，如表 8-3 所示。

表 8-3 包过滤规则示例

规　则	方　向	源　地　址	目标地址	协　议	源端口	目标端口	ACK 设置	动　作
A	出	116.111.4.0	202.108.5.6	TCP	>1023	23	任意	拒绝
B	入	202.108.5.6	116.111.4.0	TCP	23	>1023	是	任意
C	出	116.111.4.0	任意	TCP	>1023	23	任意	允许
D	入	任意	116.111.4.0	TCP	23	>1023	是	允许
E	出	116.111.4.1	任意	TCP	>1023	25	任意	允许
F	入	任意	116.111.4.1	TCP	25	>1023	是	允许
G	入	任意	116.111.4.1	TCP	>1023	25	任意	允许
H	出	116.111.4.1	任意	TCP	25	>1023	任意	允许
I	出	116.111.4.0	任意	TCP	>1023	80	任意	允许
J	入	任意	116.111.4.0	TCP	80	>1023	是	允许
K	入	98.120.8.0	116.111.4.5	TCP	>1023	80	任意	允许
L	出	116.111.4.5	98.120.8.0	TCP	80	>1023	任意	允许
M	双向	任意	任意	任意	任意	任意	任意	拒绝

规则 M 是默认项，它实现的准则是“没有明确允许就表示禁止”。

2. 代理技术

代理技术也称为应用层网关(application gateway)技术，代理(proxy)技术与包过滤技术完全不同，包过滤技术是在网络层拦截所有的信息流，代理技术是针对每一个特定应用都有一个程序。代理是企图在应用层实现防火墙的功能，代理的主要特点是有状态性。代理能提供部分与传输有关的状态，能完全提供与应用相关的状态和部分传输方面的信息，代理也能处理和管理信息。

提供代理服务的可以是一台双宿网关，也可以是一台堡垒主机，允许用户访问代理服务是很重要的，但是用户是绝对不允许注册到应用层网关中的。

3. 电路级网关技术

应用层代理为一种特定的服务(如 FTP 和 Telnet 等)提供代理服务，代理服务器不但转发流量而且对应用层协议做出解释。电路级网关(circuit level gateway)也是一种代理，但是只能是建立起一个回路，对数据包只起转发的作用。电路级网关只依赖于 TCP 连接，并不进行任何附加的包处理或过滤。

这种代理的优点是它可以对各种不同的协议提供服务，但这种代理需要改进客户程序。这种网关对外像一个代理，而对内则是一个过滤路由器。

4. 状态检查技术

防火墙仅检查独立的信息包是不够的，因为状态信息是控制新的通信连接的最基本的因素。对于某一通信连接，通信状态和应用状态是对该连接做控制决定的关键因素。因此为了保证高层的安全，防火墙必须能够访问、分析和利用以下几种信息：

- 通信信息。所有应用层的数据包的信息。
- 通信状态。以前的通信状态信息。
- 来自应用状态。其他应用的状态信息。
- 信息处理。基于以上所有元素表达式的估算。

5. 地址翻译技术

网络地址翻译(Network Address Translation，NAT)，就是将一个 IP 地址用另一个 IP 地址代替。尽管，最初设计 NAT 的目的是为了增加在专用网络中可使用的 IP 地址数，但是它有一个隐蔽的安全特性，如内部主机隐蔽等，保证了网络的安全性。

8.5 应用实例

8.5.1 “天网”软件防火墙的配置与应用技术

软件防火墙又称个人防火墙，主要用于个人网络终端。个人防火墙的主要优势在于价廉物美，花很少的钱就可以购买一份软件防火墙。

当前，软件防火墙有天网、瑞星、金山、诺顿和费尔等产品。在这里，介绍应用较为广泛的“天网个人防火墙”。

天网防火墙个人版是个人计算机使用的网络安全程序，根据管理者设定的安全规则把守网络，提供强大的访问控制、信息过滤等功能，帮助用户抵挡网络入侵和攻击，防止信息泄露。天网防火墙把网络分为本地网和互联网，可针对来自不同网络的信息，来设置不同的安全方案，适合于任何方式上网的用户。

本小节以“天网防火墙个人版 V2.50”为蓝本，介绍天网防火墙的安装、配置与应用技术。

天网防火墙个人版由 3 个可执行文件组成。

- skynet v2.50.exe。防火墙安装程序。
- 使用说明.txt。防火墙安装使用说明文件。
- 天网防火墙个人版式 V2.50 破解程序.exe。解码程序。

1. 软件安装

双击天网防火墙文件夹下的 skynet v2.50.exe，即开始安装，安装过程根据屏幕提示进行。

2. 防火墙设置向导

防火墙软件安装完毕后，自动进入“设置向导”对话框，单击“下一步”按钮，进入“安全级别设置”对话框，如图 8-5 所示。

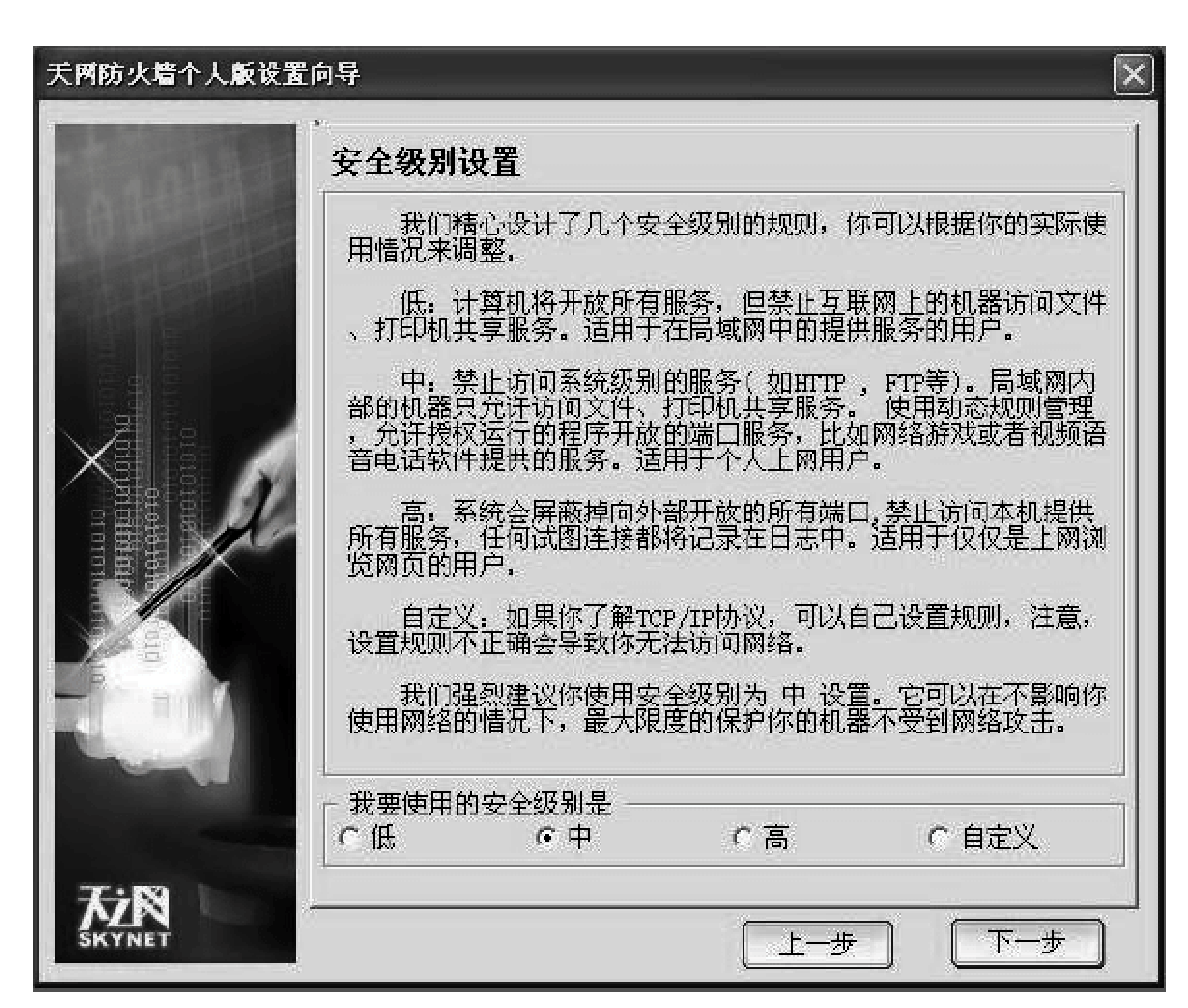


图 8-5　安全级别设置

可根据需要选择“低”、“中”、“高”或“自定义”级别，再单击“下一步”按钮。进入“局域网信息设置”对话框，如图 8-6 所示。



图 8-6 “局域网信息设置”对话框

选择“我的计算机在局域网中使用”选项，系统自动将本机的地址填入“我在局域网中的地址是”栏目中，若 IP 地址没有填入，则单击“刷新”按钮。然后单击“下一步”按钮，进入如图 8-7 所示的窗口。

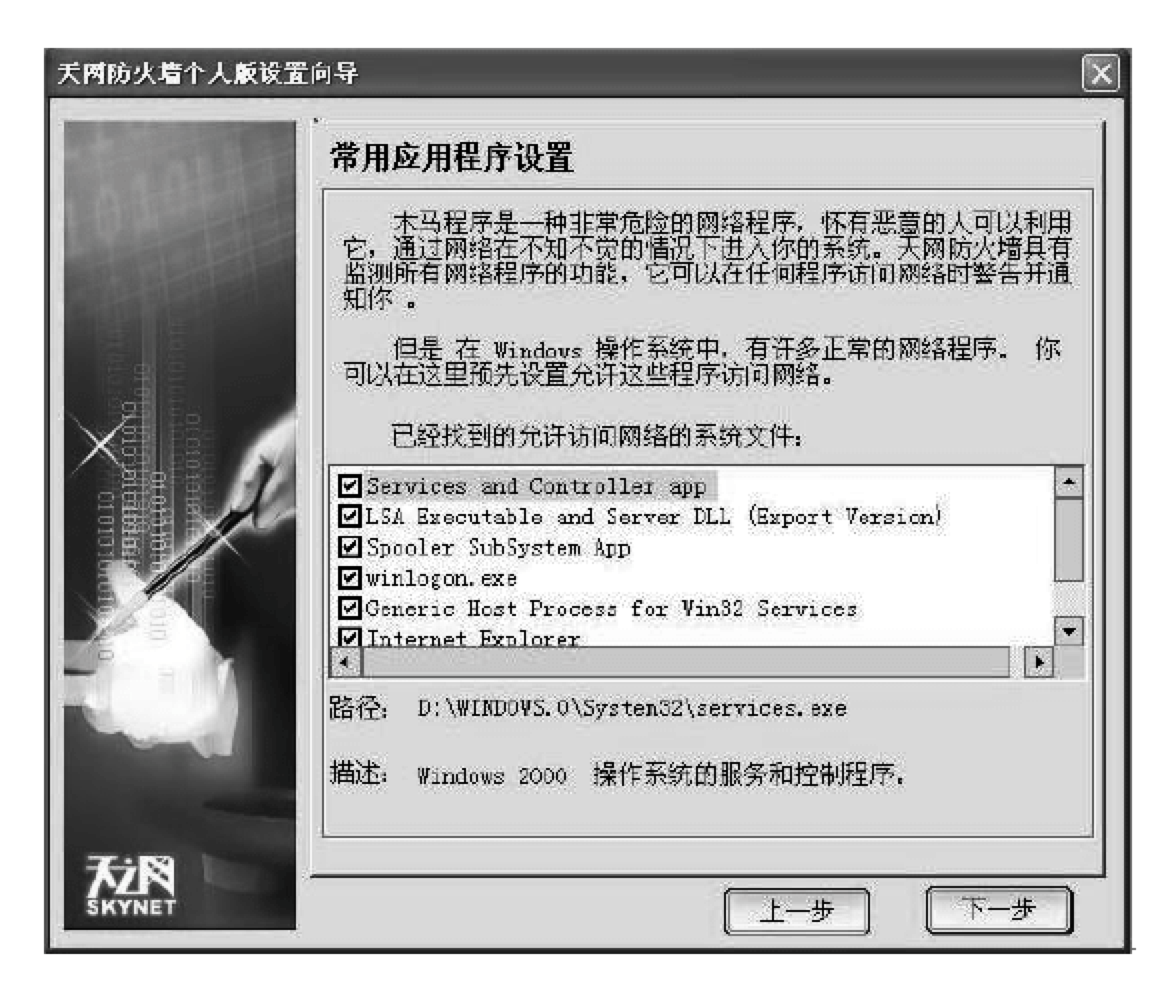


图 8-7 “常用应用程序设置”窗口

在图 8-7 所示的屏幕中，可进行应用程序的设置。应用程序设置完毕后，单击“下一步”按钮，之后根据屏幕提示操作即可。

3. 解码(打补丁)

软件安装完毕后，还要进行解码，即打补丁，解码程序文件名为“天网防火墙个人版

[正式版]V2.5 破解程序”。进入“天网防火墙”文件夹，如图 8-8 所示。



图 8-8　天网防火墙文件清单

在“天网防火墙”文件夹下选择“天网防火墙个人版[正式版]V2.5 破解程序”，单击“打开”按钮，进入“运行程序”窗口，如图 8-9 所示。

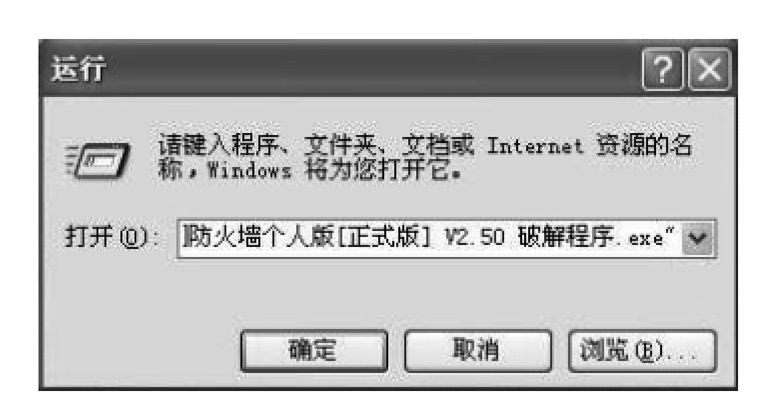


图 8-9　运行程序窗口

单击“确定”按钮，得到如图 8-10 所示的对话框。

在该窗口中，首先单击“浏览”命令，在 SkyNet 文件夹下选择文件 PFW，再单击“确定”按钮，开始解码，解码完毕，得到如图 8-11 所示的窗口。

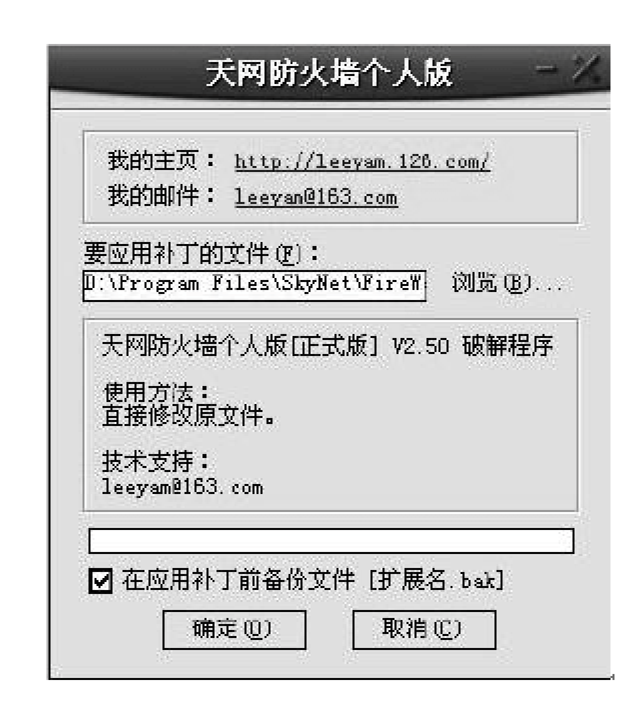


图 8-10　补丁程序运行窗口



图 8-11　解码完毕

单击"确定"按钮,解码完毕。

4. 防火墙的启动与配置

1) 防火墙的启动

在 Windows 98/2000/XP 桌面上,单击"开始"|"程序"|"天网防火墙"|"天网防火墙个人版",天网防火墙个人版即启动,得到如图 8-12 所示的屏幕。

2) 防火墙的配置

(1) 系统设置。

单击"系统设置"按钮,如图 8-12 所示标注处。



图 8-12 系统设置

选中"开机自动启动防火墙",在该选项前面将出现一个"√",以后,每次启动计算机时就会自动启动天网防火墙。

(2) 应用程序规则设置。

单击"应用程序规则设置"按钮,如图 8-13 所示标注处。

在该对话框中,可对应用程序访问权限进行设置。

(3) 自定义 IP 规则。

单击"自定义 IP 规则设置"按钮,如图 8-14 所示标注处。

在此对话框中,可对 IP 地址有关规则进行设置。

5. 天网个人防火墙的应用

天网防火墙个人版除了上述的"应用程序规则"、"自定义 IP 规则"和"系统设置"3 个配置按钮之外,还有"应用程序网络使用情况"、"日志"和"接通/断开网络"3 个应用按钮,

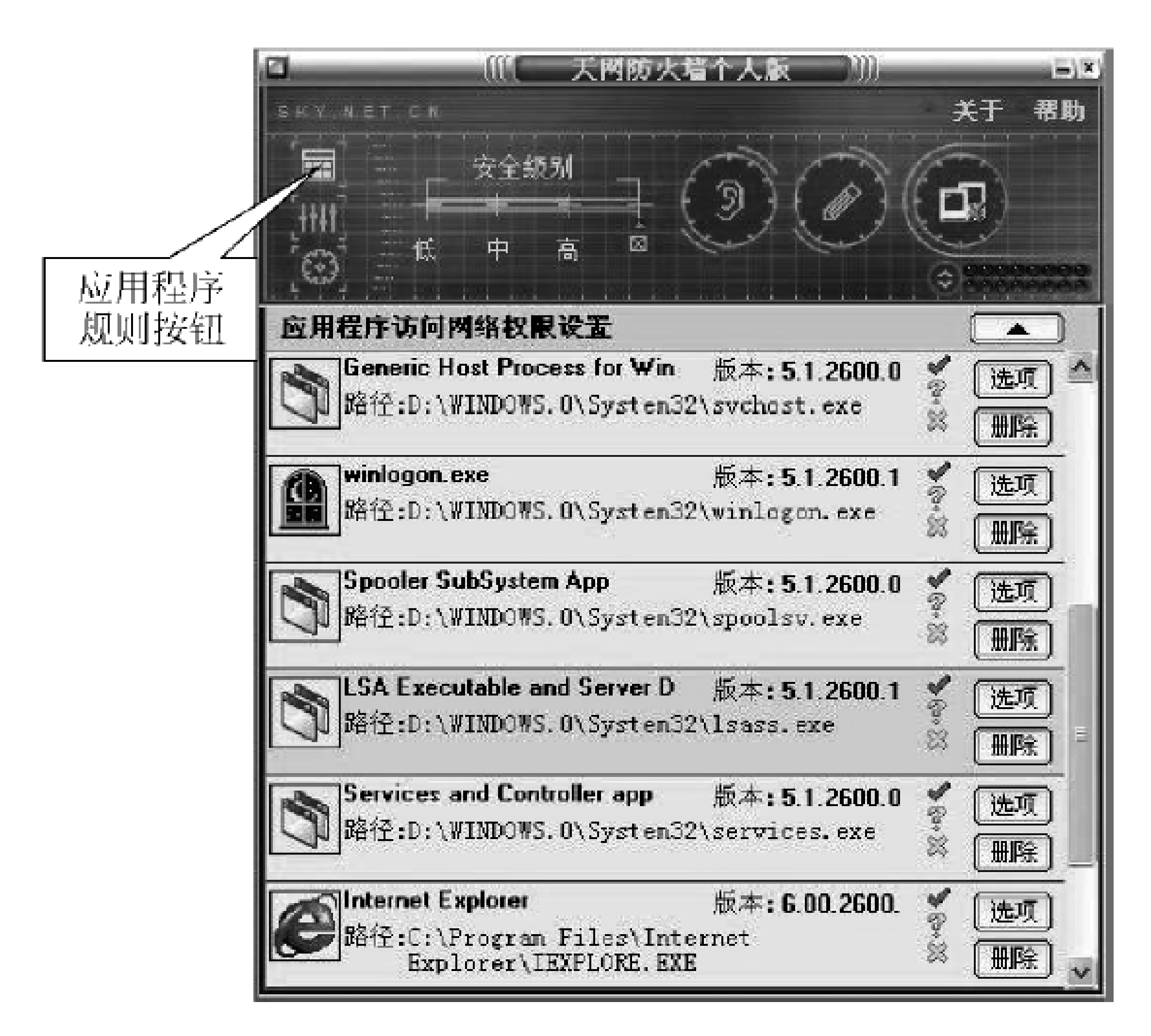


图 8-13 应用程序规则



图 8-14 自定义 IP 规则

如图 8-15 所示。

单击“应用程序使用情况”按钮，可查看应用程序访问本机的记录情况；单击“日志”按钮，可查看防火墙的工作日志；单击“接通/断开网络”按钮，可将本机与网络重新连接或断开。



图 8-15 应用按钮示意图

8.5.2 静态包过滤防火墙的配置技术

1. 静态包过滤防火墙的基本功能

静态包过滤防火墙工作在 TCP/IP 协议的 IP 层，其工作流程如图 8-16 所示。

静态包过滤防火墙的主要功能是，依据事先设定的过滤规则，检查数据流中每个数据包。根据数据包中的源地址、目标地址、端口号、数据的对话协议和数据包头中的各种标志位等因素来确定是否让该数据包通过。

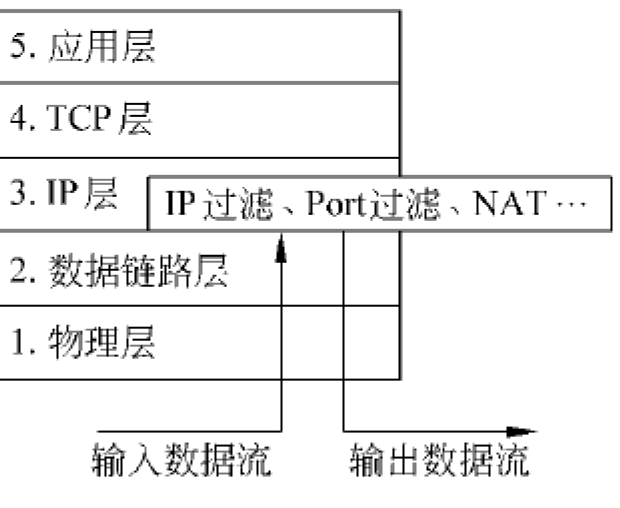


图 8-16 静态包过滤防火墙工作流程

静态包过滤防火墙的具体过滤内容如下：

- 数据包协议类型。如 TCP、UDP、ICMP 和 IGMP 等；
- 源 IP 地址。
- 目的 IP 地址。
- 源端口。FTP、HTTP、DNS 和 E-mail 等。
- 目的端口。FTP、HTTP、DNS 和 E-mail 等。
- TCP 信号选项：SYN、ACK、FIN 和 RST 等。
- 数据包流向。in 或 out。
- 数据包流经的网络接口。eth0、eth1。
- 其他协议选项。ICMP ECHO、ICMP ECHO REPLY 等。

2. 静态包过滤防火墙的配置实例

例 8-4 设内部网络 IP 地址及其端口号为 192.168.0.0/24，防火墙内部网卡 eth1 的地址为 192.168.0.1，防火墙的外部网卡地址为 10.11.12.13，DNS 地址为 10.11.15.4，其配置规则如下：

- 允许内部网络的所有主机都能访问外网的 WWW（端口号为 80）、FTP（端口号为 21）服务。
- 外部网络的所有主机不能访问内部网络。

该规则配置如下（eth0 为防火墙外部网络接口网卡）。

```
set internal=192.168.0.0/24
deny ip from $internal to any in via eth0
deny ip from not $internal to any in via eth1
allow udp from $internal to any dns
allow udp from any dns to $internal
allow tcp from any to any established
allow tcp from $internal to any www in via eth1
allow tcp from $unternal to any ftp in via eth1
allow tcp from any ftp-data to $Internal in via eth0
allow ip from any to any
```

8.5.3 状态监测防火墙的配置技术

1. 状态监测防火墙的基本功能

静态包过滤防火墙的过滤技术的一个致命缺陷在于：为了能实现期望的通信，防火墙必须保持部分端口永久性地开放，这就给攻击防火墙留下了安全隐患。为了能有效地避免和克服这一缺陷，引入了动态包过滤技术，动态包过滤防火墙也随之问世。

动态包过滤技术的主要特点是，能在数据包通过打开的端口到达目的地后，防火墙能及时关闭相应的端口。

状态包过滤技术则是在动态包过滤技术的基础上发展起来的，是对动态包过滤技术的扩展和增强。主要体现如下：

状态包过滤技术采用了一个被称之为“监测模块”的“软件引擎”（软件引擎的网络安全策略是在网关上执行的），该监测模块工作在数据链路层和网络层之间，它可对网络通信中各层实施监测分析，提取相关的通信和状态信息，并在动态连接表中进行状态及上下文信息的存储和更新，这些动态连接表会被不断地修改和更新，为下一个通信检查积累数据。

状态包过滤技术的主要优点在于：能够为基于无连接协议的应用及基于端口动态分配的协议提供安全支持，而静态包过滤技术和代理网关是不支持这类服务的。

总体来说，状态包过滤技术减少了端口的开放时间，提供了对绝大多数服务的支持，

其缺陷是允许外部主机和内部主机直接连接,也不能提供用户鉴别机制。

状态包过滤防火墙的工作流程如图 8-17 所示。

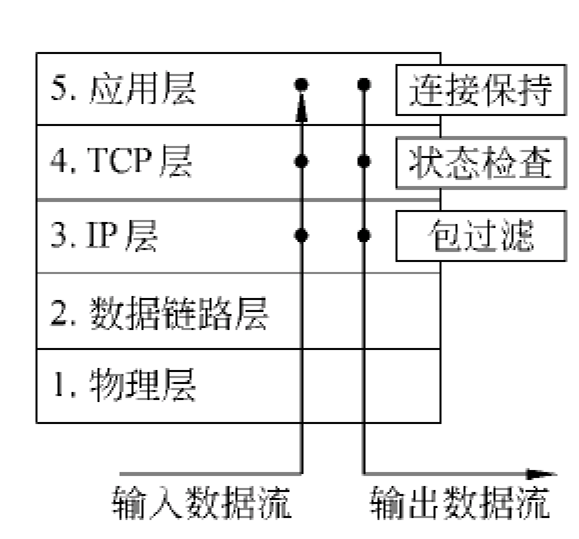


图 8-17 状态监测防火墙工作流程图

2. 状态监测防火墙的配置实例

例 8-5 设内部网络 IP 地址及其端口号为 192.168.0.0/24,防火墙内部网卡 eth1 的地址为 192.168.0.1,防火墙的外部网卡地址为 10.11.12.13,DNS 地址为 10.11.15.4,其配置规则如下:

- 允许内部网络的所有主机都能访问外网的 WWW(端口号为 80)、FTP(端口号为 21)服务。
- 外部网络的所有主机不能访问内部网络。

该规则配置如下:

```
set internal=192.168.0.0/24
deny ip from $internal to any in via eth0
deny ip from not $internal to any in via eth1
allow $internal access any dns by udp keep state
allow $internal access any www by tcp keep state
allow $internal access any ftp by tcp keep state
allow ip from any to any
```

习 题 8

1. 什么是防火墙?
2. 防火墙的基本任务是什么?
3. 什么是电路级网关?
4. 什么是堡垒主机?
5. Internet 的保留地址有哪些?
6. 网络防火墙的主要目的是什么?
7. 个人防火墙的基本功能是什么?
8. 防火墙采用的安全策略是什么?

第 9 章 chapter 9

入侵检测技术

9.1 入侵检测的基本原理

9.1.1 入侵检测的基本原理概述

1. 入侵检测产品的现状

入侵检测系统 IDS(Intrusion Detect System)分为两种,主机入侵检测系统(HIDS)和网络入侵检测系统(NIDS)。主机入侵检测系统分析对象为主机审计日志,所以需要在主机上安装入侵检测软件,针对不同的系统、不同的版本需安装不同的主机引擎,安装配置较为复杂,同时对系统的运行和稳定性造成影响,目前在国内应用较少。网络入侵监测分析对象为网络数据流,只需安装在网络的监听端口上,对网络的运行无任何影响,目前国内使用较为广泛。本章介绍的是当前广泛使用的网络入侵检测系统。

2. 入侵检测系统的作用

我们知道,防火墙是 Internet 网络上最有效的安全保护屏障,防火墙在网络安全中起到大门警卫的作用,对进出的数据依照预先设定的规则进行匹配,符合规则的就予以放行,起到访问控制的作用,是网络安全的第一道闸门。但防火墙的功能也有局限性,防火墙只能对进出网络的数据进行分析,对网络内部发生的事件完全无能为力。

同时,由于防火墙处于网关的位置,不可能对进出攻击作太多判断,否则会严重影响网络性能。如果把防火墙比作大门警卫的话,入侵检测就是网络中不间断的摄像机,入侵检测通过旁路监听的方式不间断的收取网络数据,对网络的运行和性能无任何影响,同时判断其中是否含有攻击的企图,通过各种手段向管理员报警。

入侵检测系统 IDS 是主动保护自己免受攻击的一种网络安全技术。IDS 对网络或系统上的可疑行为做出相应的反应,及时切断入侵源,保护现场并通过各种途径通知网络管理员,增强系统安全的保障。

3. 入侵检测系统的工作流程

入侵检测系统由数据收集、数据提取、数据分析和事件处理等几个部分组成,如图 9-1

所示。

1）数据收集

入侵检测的第一步是数据收集，内容包括系统、网络运行、数据及用户活动的状态和行为，而且，需要在计算机网络系统中的若干不同关键点(不同网段和不同主机)收集数据。入侵检测很大程度上依赖于收集数据的准确性与可靠性，因此，必须使用精确的软件来报告这些信息，因为黑客经常以替换软件的方式移走这些数据，例如替换被程序调用的子程序、库和其他工具。数据的收集主要来源以下几个方面，系统和网络日志文件、目录和文件不期望的改变、程序不期望的行为以及物理形式的入侵数据等。

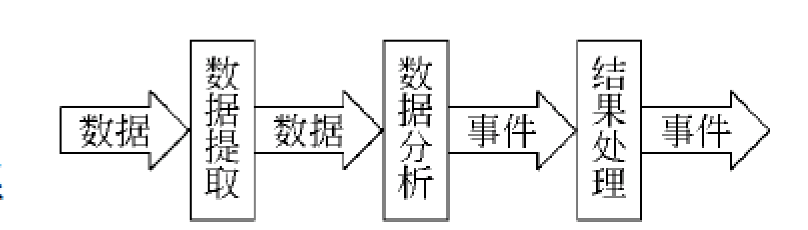


图 9-1　入侵检测系统工作流程

2）数据提取

从收集到的数据中提取有用的数据，以供数据分析之用。

3）数据分析

对收集到的有关系统、网络运行、数据及用户活动的状态和行为等数据通过三种技术手段进行分析，模块匹配、统计分析和完整性分析。

4）结果处理

记录入侵事件，同时采取报警、中断连接等措施。

9.1.2　入侵检测系统的分类

入侵检测系统(IDS)可以分成 3 类，基于主机型(host based)入侵检测系统、基于网络型(network based)入侵检测系统和基于代理型(agent based)入侵检测系统。

1. 基于主机的入侵检测系统

基于主机的入侵检测系统通常以系统日志、应用程序日志等审计记录文件作为数据源。它是通过比较这些审计记录文件的记录与攻击签名(attack signature，指用一种特定的方式来表示已知的攻击模式)以发现它们是否匹配。如果匹配，检测系统向系统管理员发出入侵报警并采取相应的行动。基于主机的 IDS 可以精确地判断入侵事件，并可对入侵事件及时做出反应。它还可针对不同操作系统的特点判断应用层的入侵事件。基于主机的 IDS 有着明显的优点。

- 适合于加密和交换环境。
- 可实时的检测和响应。
- 不需要额外的硬件。

基于主机的入侵检测系统对系统内在的结构却没有任何约束，同时可以利用操作系统本身提供的功能，并结合异常检测分析，更能准确的报告攻击行为。

基于主机的入侵检测系统存在的不足之处在于，会占用主机的系统资源，增加系统负荷，而且针对不同的操作平台必须开发出不同的程序，另外所需配置的数量众多。

2. 基于网络的入侵检测系统

基于网络的入侵检测系统把原始的网络数据包作为数据源。利用网络适配器来实时地监视并分析通过网络进行传输的所有通信业务。它用攻击识别模块进行攻击签名识别,其方法有模式、表达式或字节码匹配,频率或阈值比较,次要事件的相关性处理,统计异常检测等。一旦检测到攻击,IDS 的响应模块通过通知、报警以及中断连接等方式来对攻击行为做出反应。然而它只能监视通过本网段的活动,并且精确度较差,在交换网络环境中难于配置,防欺骗的能力也比较差。其优势有:

- 成本低。
- 攻击者转移证据困难。
- 实时检测和响应。
- 能够检测到未成功的攻击企图。
- 与操作系统无关,即基于网络的 IDS 并不依赖主机的操作系统作为检测资源。

3. 基于代理的入侵检测系统

基于代理的入侵检测系统用于监视大型网络系统。随着网络系统的复杂化和大型化,系统弱点趋于分布式,而且攻击行为也表现为相互协作式特点,所以不同的 IDS 之间需要共享信息,协同检测。整个系统可以由一个中央监视器和多个代理组成。中央监视器负责对整个监视系统的管理,它应该处于一个相对安全的地方。代理则被安放在被监视的主机上(如服务器、交换机和路由器等)。代理负责对某一主机的活动进行监视,如收集主机运行时的审计数据和操作系统的数据信息,然后将这些数据传送到中央监视器。代理也可以接受中央监控器的指令,这种系统的优点是可以对大型分布式网络进行检测。

9.1.3 入侵检测技术的发展方向

可以看到,在入侵检测技术发展的同时,入侵技术也在不断更新,攻击者已将如何绕过 IDS 或攻击 IDS 系统作为研究重点。高速网络,尤其是交换技术的发展以及通过加密信道的数据通信,使得通过共享网段侦听的网络数据采集方法显得不足,而大量的通信量对数据分析也提出了新的要求。随着信息系统对一个国家的社会生产与国民经济的影响越来越重要,信息战已逐步被各个国家重视,信息战中的主要攻击“武器”之一就是网络的入侵技术,信息战的防御主要包括“保护”、“检测”与“响应”,入侵检测则是其中“检测”与“响应”环节不可缺少的部分。对入侵检测技术主要的发展方向有下列几个方向。

- 分布式入侵检测与通用入侵检测架构 CIDF(Common Intrusion Detection Framework)。传统的 IDS 一般局限于单一的主机或网络架构,对异构系统及大规模网络的监测明显不足。同时不同的 IDS 系统之间不能协同工作,为解决这一问题,需要分布式入侵检测技术与通用入侵检测架构。CIDF 以构建通用的 IDS 体系结构与通信系统为目标,GrIDS(Graph-based Intrusion Detection System,基于曲线入侵

检测系统)跟踪与分析分布系统入侵以及实现在大规模的网络与复杂环境中的入侵检测。

- 应用层入侵检测。许多入侵的语义只有在应用层才能理解,而目前的 IDS 仅能检测如 Web 之类的通用协议,而不能处理如 Lotus Notes、数据库系统等其他的应用系统。许多基于客户、服务器结构与中间件技术及对象技术的大型应用,需要应用层的入侵检测保护。另外,基于 CORBA(Common Object Request Broker Architecture)环境下的 IDS 也是一个重要的发展方向。
- 智能的入侵检测。入侵方法越来越多样化与综合化,尽管已经有智能体、神经网络与遗传算法在入侵检测领域应用研究,但是这只是一些尝试性的研究工作,需要对智能化的 IDS 加以进一步的研究以解决其自学习与自适应能力。
- 入侵检测的评测方法。用户需对众多的 IDS 系统进行评价,评价指标包括 IDS 检测范围、系统资源占用、IDS 系统自身的可靠性。从而设计通用的入侵检测测试与评估方法和平台,实现对多种 IDS 系统的检测已成为当前 IDS 的另一重要研究与发展领域。
- 全面的安全防御方案。即使用安全工程风险管理的思想与方法来处理网络安全问题,将网络安全作为一个整体工程来处理。从管理、网络结构、加密通道、防火墙、病毒防护和入侵检测多方位全面对所关注的网络作全面的评估,然后提出可行的全面解决方案。
- B/S 结构的入侵检测。目前使用的 C/S 结构软件(即客户机/服务器模式)分为客户机和服务器两层,客户机不是毫无运算能力的输入、输出设备,而是具备了一定的数据处理和数据存储能力,通过把应用软件的计算和数据合理地分配在客户机和服务器两端,可以有效地降低网络通信量和服务器运算量。由于服务器连接数量和数据通信量的限制,这种结构的软件适于在用户数目不多的局域网内使用。B/S 结构软件(浏览器/服务器模式)是随着 Internet 技术的兴起,对 C/S 结构的一种改进。在这种结构中,软件应用的业务逻辑完全在应用服务器端实现,用户表现完全在 Web 服务器实现,客户端只需要浏览器即可进行业务处理,是一种全新的软件系统构造技术。这种结构已经成为当今应用软件的首选体系结构。
- 智能关联。智能关联是将企业相关系统的信息(如主机特征信息)与网络 IDS 检测结构相融合,从而减少误警。如系统的脆弱性信息需要包括特定的操作系统(OS)以及主机上运行的服务。当 IDS 使用智能关联时,它可以参考目标主机上存在的、与脆弱性相关的所有告警信息。如果目标主机不存在某个攻击可以利用的漏洞,IDS 将抑制告警的产生。智能关联包括主动关联和被动关联。主动关联是通过扫描确定主机漏洞,被动关联是借助操作系统的指纹识别技术,即通过分析 IP、TCP 报头信息识别主机上的操作系统。
- 告警泛滥抑制。IDS 产品使用告警泛滥抑制技术可以降低误警率。在利用漏洞的攻击势头逐渐变强之时,IDS 短时间内会产生大量的告警信息,而 IDS 传感器却要对同一攻击重复记录,尤其是蠕虫在网络中自我繁殖的过程中,这种现象最为严重。这种现象为“告警饱和”。所谓“告警泛滥”是指短时间内产生的关于同

一攻击的告警。下一代 IDS 产品利用一些规则(规则的制定需要考虑传感器)筛选产生的告警信息来抑制告警泛滥;IDS 可根据用户需求减少或抑制短时间内同一传感器针对某个流量产生的重复告警。这样,网管人员可以专注于公司网络的安全状况,不至于为泛滥的告警信息大伤脑筋。告警泛滥抑制技术是将一些规则或参数(包括警告类型、源 IP、目的 IP 以及时间窗大小)融入到 IDS 传感器中,使传感器能够识别告警饱和现象并实施抑制操作。有了这种技术,传感器可以在告警前对警报进行预处理,抑制重复告警。例如,可以对传感器进行适当配置,使它忽略在 30 秒内产生的针对同一主机的告警信息;IDS 在抑制告警的同时可以记录这些重复警告用于事后的统计分析。

- 告警融合。该技术是将不同传感器产生的、具有相关性的低级别告警融合成更高级别的警告信息,这有助于解决误报和漏报问题。当与低级别警告有关的条件或规则满足时,安全管理员在 IDS 上定义的元告警相关性规则就会促使高级别警告产生。如扫描主机事件,如果单独考虑每次扫描,可能认为每次扫描都是独立的事件,而且对系统的影响可以忽略不计;但是,如果把在短时间内产生的一系列事件整合考虑,会有不同的结论。IDS 在 10min 内检测到来自于同一 IP 的扫描事件,而且扫描强度在不断升级,安全管理人员可以认为是攻击前的渗透操作,应该作为高级别告警对待。这个例子告诉我们告警融合技术可以发出早期攻击警告,如果没有这种技术,需要安全管理员来判断一系列低级别告警是否是随后更高级别攻击的先兆;而通过设置元警告相关性规则,安全管理员可以把精力都集中在高级别警告的处理上。
- 可信任防御模型。改进的 IDS 中应该包含可信任防御模型的概念。2004 年多数传统的 IDS 供应商已经逐渐地把防御功能加入到 IDS 产品中。与此同时,IPS(入侵防御系统)产品的使用率在增长,但是安全人士仍然为 IDS 产品预留了实现防御功能的空间。IDS 产品供应商之所以这样做,部分原因在于他们认识到防御功能能否有效地实施关键在于检测功能的准确性和有效性。没有精确的检测就谈不上建立可信任的防御模型;所以,开发出好的内嵌防御功能的 IDS 产品关键在于提高检测的精确度。在下一代 IDS 产品中,融入可信任防御模型后,将会对第一代 IPS 产品遇到的问题(误报导致合法数据被阻塞、丢弃;自身原因造成的拒绝服务攻击泛滥;应用级防御)有个圆满的解决。

可信任防御模型中采用的机制如下:

(1) 信任指数。IDS 为每个告警赋予一个可信值,即在 IDS 正确评估攻击/威胁后对是否发出告警的自我确信度。如对于已知的 SQLSlammer 攻击,IDS 在分析数据流中的数据报类型和大小后,以高确信度断定数据流包含 SQLSlammer 流量。因为这种攻击使用 UDP,数据报大小为 376,所用端口为 1434;有了这样的数据,IDS 会为相应的告警赋予高信任指数。

(2) 拒绝服务攻击(DOS)。攻击者可能冒充内网 IP(如邮件服务器 IP)进行欺骗攻击,传统防御系统将会拒绝所有来自邮件服务器的流量,导致网内机器不能接受外部发来的邮件,下一代 IDS 产品能够识别这种自发的 DOS 情形,并且降低发生概率。

（3）应用级攻击。这是一种针对被保护力度低的应用程序（如即时通信工具、VoIP等）发起的攻击，攻击造成的后果非常严重。下一代IDS产品提供深度覆盖技术来保护脆弱的应用程序免遭攻击。

9.2 网络入侵技术

网络入侵检测的技术主要有异常检测模型和误用检测模型，此外，还有基于生物免疫系统的入侵检测模型和基于伪装的入侵检测模型。

9.2.1 基本检测方法

1. 基于用户特征的检测

基于用户特征的检测方法是根据用户通常的举动来识别特定的用户，用户的活动模式根据在一段时间内的观察后建立。例如，某个用户多次使用某些命令，在特定的时间内以一定的频度访问文件、系统登录及执行相同的程序等。可以按照用户的活动情况给每个合法的用户建立特征库，用以检测和判断登录用户的合法性，因为非法用户不可能像合法用户一样地进行同样的操作。

2. 基于入侵者的特征的检测

当外界用户或入侵者试图访问某个计算机系统时会进行某些特殊的活动或使用特殊方法，如果这些活动能够予以描述并作为对入侵者的描述，入侵活动就能够被检测到。非法入侵者活动的一个典型例子是，当其获得系统的访问权时，通常会立即查看当前有哪些用户在线，并且会反复检查文件系统和浏览目录结构，还会打开这些文件，另外，非法入侵者在一个系统上不会停留过久，而一个合法的用户一般是不会这样做的。

3. 基于活动的检测

一般来说，非法入侵者在入侵系统时会进行某些已知的且具有共性的操作，比如在入侵UNIX时入侵通常要试图获得根（root）权限，所以，用户有理由认为任何企图获得根权限的活动都要被检测。

9.2.2 异常检测模型

1. 异常检测模型的基本原理

异常检测，也被称为基于行为的检测。其基本前提是假定所有的入侵行为都是异常的。其基本原理是，首先建立系统或用户的“正常”行为特征轮廓，通过比较当前的系统或用户的行为是否偏离正常的行为特征轮廓来判断是否发生了入侵。而不是依赖于具体行为是否出现来进行检测的，从这个意义上来讲，异常检测是一种间接的方法。

2. 异常检测的关键技术

1）特征量的选择

异常检测首先是要建立系统或用户的“正常”行为特征轮廓，这就要求在建立正常模型时，选取的特征量既要能准确地体现系统或用户的行为特征，又能使模型最优化，即以最少的特征量就能涵盖系统或用户的行为特征。例如，可以检测磁盘的转速是否正常，CPU 是否无故超频等异常现象。

2）参考阈值的选定

因为在实际的网络环境下，入侵行为和异常行为往往不是一对一的等价关系，经常发生这样的异常情况，如某一行为是异常行为，而它并不是入侵行为；同样存在某一行为是入侵行为，而它却并不是异常行为的情况。这样就会导致检测结果的虚警（false positives）和漏警（false negatives）的产生。由于异常检测是先建立正常的特征轮廓作为比较的参考基准，这个参考基准即参考阈值的选定是非常关键的，阈值定的过大，那漏警率会很高；阈值定的过小，则虚警率就会提高。合适的参考阈值的选定是影响这一检测方法准确率的至关重要的因素。

从异常检测的原理可以看出，该方法的技术难点在于“正常”行为特征轮廓的确定、特征量的选取、特征轮廓的更新。由于这几个因素的制约，异常检测的虚警率很高，但对于未知的入侵行为的检测非常有效。此外，由于需要实时地建立和更新系统或用户的特征轮廓，这样所需的计算量很大，对系统的处理性能要求会很高。

3. 异常检测模型的实现方法

异常检测模型常用的实现方法有统计异常检测方法、基于特征选择异常检测方法、基于贝叶斯推理异常检测方法、基于贝叶斯网络异常检测方法、基于模式预测异常检测方法、基于神经网络异常检测方法、基于机器学习异常检测方法和基于数据采掘异常检测方法等。

1）基于统计分析的异常检测方法

基于统计分析的异常检测方法是根据异常检测器观察主体的活动情况，随之产生能刻画这些活动的行为框架。每一个框架能保存记录主体的当前行为，并定时地将当前的框架与存储的框架合并。通过比较当前的框架与事先存储的框架来判断异常行为，从而检测出网络的入侵行为。

设 $M_1, M_2, \cdots, M_n$ 为框架的特征变量，如 CPU 的使用、I/O 的使用、使用地点及时间、邮件的使用、文件的访问数量、网络的会话时间等。用 $S_1, S_2, \cdots, S_n$ 分别表示与框架中的变量 $M_1, M_2, \cdots, M_n$ 对应的异常测量值，这些值表明了异常程度，S_i 的值越高，则 M_i 的异常性就越大。

框架的异常值是将有关的异常测量平方加权后得到的，其计算式如下：

$$S = a_1 S_1^2 + a_2 S_2^2 + \cdots + a_n S_n^2$$

其中，a_i 表示框架与变量 M_i 相关的权重，一般地，$M_1, M_2, \cdots, M_n$ 不是相互独立的，而是具有相关性的。常见的几种异常测量值的测量类型如下：

- 活动强度测量。用以描述活动的处理速度。
- 审计记录分布测量。用以描述最近审计记录中所有活动类型的分布状况。
- 类型测量。用以描述特定的活动在各种类型的分布状况。
- 顺序测量。用以描述活动的输出结果。

2）基于特征选择的异常检测方法

基于特征选择的异常检测方法是通过从一组度量中挑选能检测出入侵的度量构成子集来准确地预测或分类已检测到的入侵。

3）基于贝叶斯推理的异常检测方法

基于贝叶斯(Bayesian)推理异常检测方法是通过在任意的时刻，测量 $A_1, A_2, \cdots, A_n$ 变量值推理判断系统是否有入侵事件的发生。其中每个 A_i 变量表示系统不同的方面特征(如磁盘 I/O 的活动数量，或者系统中页面出错的次数等)。

4）基于贝叶斯网络的异常检测方法

基于贝叶斯网络的异常检测方法是通过建立起异常入侵检测的贝叶斯网络，然后将其用作分析异常测量的结果。

5）基于模式预测的异常检测方法

基于模式预测异常检测方法是假设事件序列不是随机的而是能遵循可辨别的模式，这种检测方法的主要特点是考虑事件的序列及其相互联系。其典型模型是由 Teng 和 Chen 提出的基于时间的推理方法，利用时间规则识别用户行为正常模式的特征。通过归纳学习产生这些规则集，并能动态地修改系统中的这些规则，使之具有高的预测性、准确性和可信度。

6）基于神经网络的异常检测方法

基于神经网络的入侵检测方法是训练神经网络连续的信息单元，这里的信息单元指的是一条命令。网络的输入层是用户当前输入的命令和已执行过的 N 条命令，神经网络就是利用用户使用过的 N 条命令来预测用户可能使用的下一条命令。当神经网络预测不出某用户正确的后续命令，即在某种程度上表明了有异常事件发生，以此进行异常入侵的检测。

7）基于贝叶斯聚类的异常检测方法

基于贝叶斯聚类的异常检测方法是通过在数据中发现不同类别的数据集合，这些类反映出了基本的因果关系，以此就可以区分异常用户类，进而推断入侵事件发生来检测异常入侵的行为。

8）基于机器自学习系统的异常检测方法

基于机器自学习系统的异常检测方法是将异常检测问题归结为根据离散数学临时序列学习获得个体、系统和网络的行为特征，提出一个基于相似度的学习方法 IBL，该方法通过新的序列相似度的计算，将原始数据转化成可度量的空间。然后，应用 IBL 的学习技术和一种新的基于序列的分类方法，从而发现异常类型事件，以此进行入侵行为的检测。

9）基于数据采掘技术的异常检测方法

基于数据采掘技术的异常检测方法是将数据采掘技术应用到入侵检测研究领域中，从

审计数据或数据流提取感兴趣的知识、规则、规律和模式等形式，并用这些知识去检测异常入侵和已知的入侵。基于数据采掘技术的异常入侵检测通常使用的是 KDD(Knowledge Discovery in Databases，数据库中的知识提取)算法，该算法就是从数据库中自动提取有用的信息(知识)。这种算法的优点是选用于处理大量的数据，但 KDD 算法只能对事后数据进行分析，而不能进行实时跟踪处理。

9.2.3 误用检测模型

1. 误用检测模型的基本原理

在介绍基于误用的入侵检测的概念之前，有必要对误用的概念做一个简单的介绍。误用是英文 Misuse 的中文直译，其意思是“可以用某种规则、方式或模型表示的攻击或其他安全相关行为”。

根据对误用概念的这种理解，可以定义基于误用的入侵检测技术的含义，“误用检测技术主要是通过某种方式预先定义入侵行为，然后监视系统的运行，并从中找出符合预先定义规则的入侵行为”。

一个典型的基于误用的入侵检测系统如图 9-2 所示。

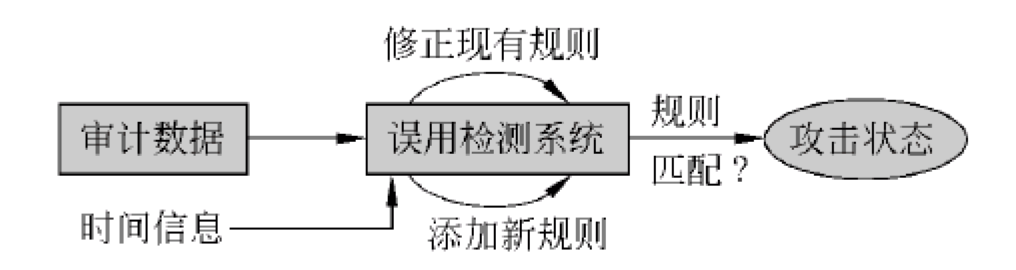


图 9-2 典型的基于误用的入侵检测系统模型

基于误用的入侵检测系统通过使用某种模式或者信号标识表示攻击，进而发现相同的攻击。这种方式可以检测许多甚至全部已知的攻击行为，但是对于未知的攻击手段却无能为力，这一点和病毒检测系统类似。

对于误用检测系统来说，最重要的技术如下：

- 如何全面描述攻击的特征，覆盖在此基础上的变种方式。
- 如何排除其他带有干扰性质的行为，减少误报率。

误用检测，也被称为基于知识的检测。其基本前提是假定所有可能的入侵行为都能被识别和表示。其原理是，首先对已知的攻击方法进行攻击签名(攻击签名是指用一种特定的方式来表示已知的攻击模式)表示，然后根据已经定义好的攻击签名，通过判断这些攻击签名是否出现来判断入侵行为的发生与否。这种方法是直接判断攻击签名的出现与否来判断入侵的，从这一点来看，它是一种直接的方法。

误用检测技术的关键问题是攻击签名的正确表示。误用检测是根据攻击签名来判断入侵的，如何用特定的模式语言来表示这种攻击行为，是该方法的关键所在。尤其是攻击签名必须能够准确地表示入侵行为及其所有可能的变种，同时又不会把非入侵行为包含进来。由于大部分的入侵行为是利用系统的漏洞和应用程序的缺陷进行攻击的，那么通过分析攻击过程的特征、条件、排列以及事件间的关系，就可具体描述入侵行为的迹

象。这些迹象不仅对分析已经发生的入侵行为有帮助，而且对即将发生的入侵也有预警作用，因为只要部分满足这些入侵迹象就意味着有入侵行为发生的可能。

误用检测是通过将收集到的信息与已知的攻击签名模式库进行比较，从而发现违背安全策略的行为。该方法类似于病毒检测系统，其检测的准确率和效率都比较高。而且这种技术比较成熟，国际上一些顶尖的入侵检测系统都采用该方法，该方法也存在一些缺点：

（1）不能检测未知的入侵行为。由于其检测机理是对已知的入侵方法进行模式提取，对于未知的入侵方法由于缺乏认识就不能进行有效的检测。也就是说漏警率比较高。

（2）与系统的相关性很强。由于不同的操作系统的实现机制不同，对其攻击的方法也不尽相同，很难定义出统一的模式库。另外由于已知认识的局限性，难以检测出内部人员的蓄意破坏和攻击行为，如合法用户的泄漏。

2. 误用入侵检测模型的基本方法

误用检测模型常用的检测方法有基于条件概率误用入侵检测方法、基于专家系统误用入侵检测方法、基于状态迁移分析误用入侵检测方法、基于键盘监控误用入侵检测方法和基于模型误用入侵检测方法等。

1）基于条件概率的误用入侵检测方法

基于条件概率的误用入侵检测方法是将入侵的方式对应于一个事件序列，并通过对事件发生的情形的分析和观察来推测入侵的一种方法。这种方法的依据是根据贝叶斯定理(Bayesian principles)进行推理检测入侵行为。

基于条件概率的误用入侵检测模型是用下面的计算公式来计算的。

$$P(\mathrm{Intrusion}|\mathrm{ES})=P(\mathrm{ES}|\mathrm{Intrusion})\frac{P(\mathrm{Intrusion})}{P(\mathrm{ES})}$$

而

$$P(\mathrm{ES})=(P(\mathrm{ES}|\mathrm{Intrusion})-P(\mathrm{ES}|\neg\mathrm{Intrusion}))\times P(\mathrm{Intrusion})+P(\mathrm{ES}|\neg\mathrm{Intrusion})$$

其中 ES 为事件序列，$P(\mathrm{ES})$为事件发生的概率，Intrusion 为一具体的事件，$P(\mathrm{Intrusion})$为事件 Intrusion 在事件序列 ES 上发生的先验概率，$P(\mathrm{ES}|\mathrm{Intrusion})$为事件 Intrusion 在事件序列 ES 上发生的后验概率，$P(\mathrm{ES}|\neg\mathrm{Intrusion})$为非 Intrusion 事件在事件序列 ES 上发生的后验概率。所谓的“先验概率”是用概率来描述人们事先对所研究对象的发生概率的估算，即根据古典概率的定义，用数学分析进行计算得到的概率。所谓的“后验概率”就是根据具体的事件资料、先验概率、特定的判别规则所计算机出来的概率，换句话说，后验概率是对先验概率进行修正后的结果。

通常，先验概率 $P(\mathrm{Intrusion})$是由网络安全管理员事先给出的，而通过对入侵报告数据的统计分析可得到 $P(\mathrm{ES}|\mathrm{Intrusion})$和 $P(\mathrm{ES}|\neg\mathrm{Intrusion})$。

2）基于专家系统的误用入侵检测方法

基于专家系统的误用入侵检测模型是通过将安全专家的经验知识表示成 if-then 规则而形成的专家知识库，然后，运用推理算法进行入侵行为的检测。

基于专家系统的误用入侵检测系统的典型模型是 CLIPS 模型，在该模型中，将入侵知识进行编码表示成 if-then 规则，并根据相应的审计跟踪事件的断言事实。编码规则说明攻击的必需条件作为 if 的组成部分。当规则的左边的条件全都满足时，规则右边的动作才会执行。

在基于专家系统的入侵检测模型中，要处理大量的数据和依赖于审计跟踪的次序。其推理方法有两种。

- 根据给定的数据，应用符号推理出入侵行为的发生。
- 根据其他的入侵证据，进行不确定性的推理。

3）基于状态迁移分析的误用入侵检测方法

状态迁移分析方法是将攻击表示成一系列被监控的系统状态迁移。攻击模式的状态对应于系统的状态，并且具有迁移到另外状态的特性，然后通过弧线连续的状态连接起来表示状态改变所需要的事件。

4）基于键盘监控的误用入侵检测方法

基于键盘监控系统的误用入侵检测方法是假设入侵者对应的击键序列模式，然后监测用户击键模式，并将这一击健模式与入侵检测模式相匹配，以检测入侵行为。

5）基于模型的误用入侵检测方法

基于模型的误用入侵检测方法是通过建立误用证据模型，根据证据推理来作出误用发生判断结论。

9.2.4 异常检测模型和误用检测模型的比较

异常检测系统试图发现一些未知的入侵行为，而误用检测系统则是检测一些已知的入侵行为。

异常检测指根据使用者的行为或资源使用状况来判断是否入侵行为的发生，而不依赖于具体行为是否出现来检测；而误用检测系统则大多是通过对一些具体的行为的判断和推理，从而检测出入侵行为。

异常检测的主要缺陷在于误检率很高，尤其在用户数目众多或工作行为经常改变的环境中；而误用检测系统由于依据具体特征库进行判断，准确度要高很多。

异常检测对具体系统的依赖性相对较小；而误用检测系统对具体的系统依赖性很强，移植性不好。

9.2.5 其他入侵检测模型

1. 基于生物免疫的入侵检测方法

生物免疫系统对外部入侵病原可自动进行抵御并可对自身进行保护，一旦抵御了某种病原体的攻击后，则可对该病原体产生抗体，即自动获得免疫功能，当该病原体再次入侵时，即可迅速进行有效的抵抗。以人为例，若某人不幸感染了结核病，治愈后，他就对结核病菌产生了抗体，以后就再也不会感染结核病了。

基于生物免疫的入侵检测系统就是通过模仿生物有机体的免疫能力，使得受保护的

系统能够将外来的非法攻击行为与自我合法行为区分开来，除了能够进行相应的处理以外，能对入侵的行为进行详细的“记忆”（即自我“学习”方法），当下一次再次出现这种攻击时，即可迅速进行抵御，以达到自我保护的目的。

事实上，基于生物免疫系统的入侵检测方法是将异常入侵检测方法与误用入侵检测方法进行有机的结合。这种方法的新颖之处在于将生物学的免疫原理应用到计算机网络的安全保护领域之中。

2. 基于伪装的入侵检测方法

基于伪装的入侵检测方法是通过在网络主机上构造或设置一些虚假的信息，并将这些信息暴露在网上，若非法入侵者对这些信息感兴趣，反复访问这些数据，或反复打开相关的文件，或下载这些文件，就可以断定系统已受到入侵攻击，并可确定当前登录者就是非法入侵者。这一技术又可称作是“蜜罐”诱骗技术。

3. 基于统计学方法的入侵检测系统

基于统计的检测规则认为入侵行为应该符合统计规律。例如，系统可以认为一次密码尝试失败并不算是入侵行为，因为的确可能是合法用户输入失误，但是如果在一分钟内有3次以上同样的操作就不可能完全是输入失误了，而可以认定是入侵行为。因此，组成分析策略的检测规则就是表示行为频度的阈值，通过检测出行为并统计其数量和频度就可以发现入侵。

统计模型常用于对异常行为的检测，在统计模型中常用的测量参数包括审计事件的数量、间隔时间和资源消耗情况等。目前，可用于入侵检测的统计模型有5种。

- 操作模型。该模型假设异常可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验值或一段时间内的统计平均得到，举例来说，在短时间内的多次失败的登录很可能是口令尝试攻击。
- 方差。计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时表明有可能是异常。
- 多元模型。操作模型的扩展，通过同时分析多个参数实现检测。
- 马尔柯夫过程模型。将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，若对应于发生事件的状态矩阵中转移概率较小，则该事件可能是异常事件。
- 时间序列分析。将事件计数与资源耗用根据时间排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是入侵。

入侵检测的统计分析首先计算用户会话过程的统计参数，再进行与阈值比较处理与加权处理，最终通过计算其“可疑”概率分析其为入侵事件的可能性。统计方法的最大优点是它可以“学习”用户的使用习惯，从而具有较高检出率与可用性。但是它的“学习”能力也给入侵者以机会，他们通过逐步“训练”使入侵事件符合正常操作的统计规律，从而透过入侵检测系统。

4. 基于专家系统的入侵检测方法

基于专家系统的入侵检测方法与运用统计方法与神经网络对入侵进行检测的方法不同，用专家系统对入侵进行检测，经常是针对有特征的入侵行为。

所谓的规则，即是知识。不同的系统与设置具有不同的规则，且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。特征入侵的特征抽取与表达，是入侵检测专家系统的关键。将有关入侵的知识转化为 if-then 结构（也可以是复合结构），if 部分为入侵特征，then 部分是系统防范措施。

运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性，建立一个完备的知识库对于一个大型网络系统往往是不可能的，且如何根据审计记录中的事件，提取状态行为与语言环境也是较困难的。

由于专家系统的不可移植性与规则的不完备性。现已不宜单独用于入侵检测，或单独形成商品软件。较适用的方法是将专家系统与采用软计算方法技术的入侵检测系统结合在一起，构成一个以已知的入侵规则为基础，可扩展的动态入侵事件检测系统，自适应地进行特征与异常检测，实现高效的入侵检测及其防御。

9.3 应用实例

9.3.1 Snort 软件简介

Snort 是一个用 C 语言编写的开放源代码软件，Snort 实际上是一个基于 libpcap（基于 UNIX/Linux 环境的网络数据包捕获函数包）的网络数据包嗅探器和日志记录工具，可以用于入侵检测。从入侵检测分类上来看，Snort 应该算是一个基于网络和误用入侵检测软件。

Snort v2.0 Snort 为开放源代码入侵检测系统软件，为用来监视网络传输量的网络型入侵检测系统。主要工作是捕捉流经网络的数据包，一旦发现与非法入侵的组合一致，便向管理员发出警告。

Snort 采用基于规则的网络信息搜索机制，对数据包进行内容的模式匹配，从中发现入侵和探测行为，例如 buffer overflows、stealth port scans、CGI attacks 和 SMB probes 等。Snort 具有实时报警的能力，它的警报信息可以发往 syslog、Server Message Block（SMB）、WinPopup messages 或者单独 alert 文件。Snort 可以通过命令进行交互，并对可选的 BPF（Berkeley Packet Filter）命令进行配置。

Snort 安装在一台主机上可对整个网络进行监视，其典型运行环境如图 9-3 所示。

Snort 由 3 个重要的子系统构成，数据包解码器、检测引擎及日志与报警系统。

1. 数据包解码器

数据包解码器主要是对各种协议栈上的数据包进行解析、预处理，以便提交给检测引擎进行规则匹配。解码器运行在各种协议栈之上，从数据链路层到传输层，最后到应

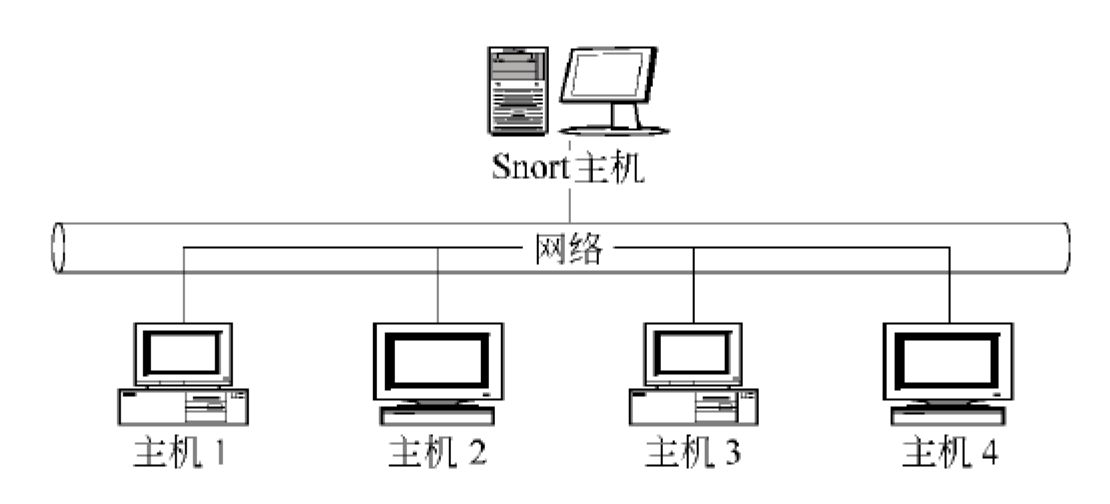


图 9-3 Snort 的典型运行环境

用层。因为当前网络中的数据流速度很快,如何保障较高的速度是解码器子系统中的一个重点。目前,Snort 解码器支持的协议包括 Ethernet、SLIP 和 raw(PPP)data-link 等。

2. 检测引擎

Snort 用一个二维链表存储它的检测规则,其中一维称为规则头,另一维称为规则选项。规则头中放置的是一些公共的属性特征,而规则选项中放置的是一些入侵特征。为了提高检测速度,通常把最常用的源/目的 IP 地址和端口信息放在规则头链表中,而把一些独特的检测标志放在规则选项链表中。规则匹配查找采用递归的方法进行,检测机制只针对当前已经建立的链表选项进行检测。当数据包满足一个规则时,就会触发相应的操作。Snort 的检测机制非常灵活,用户可以根据自己的需要很方便地在规则链表中添加所需要的规则模块。

3. 日志和报警子系统

日志和报警子系统可以在运行 Snort 的时候以命令行交互的方式进行选择。

Snort 是一种基于网络的入侵检测系统,Snort 的规则在逻辑上分为两部分,规则头(rule header)和规则选项(rule option)。规则头定义了规则的行为、所匹配网络报文的协议、源地址、目标地址及其网络掩码、源端口和目标端口等信息;规则选项部分则包含了所要显示给用户查看的警告信息,以及用来判定此报文是否为攻击报文的其他信息。

9.3.2 Snort 软件的使用技术

Snort 软件使用的技术如下:

- 网络安全事件响应技术。
- 安全事件的定义。
- 事件响应的处理过程。
- 网络攻击的追踪。
- 应急处置与恢复技术。
- 远程备份技术。
- 安全事件的定义。

所谓"事件",指的是那些影响计算机系统和网络安全的不当行为。这些行为包括在计算机和/网络上发生的可以观察得到的任何现象,包括通过网络连接到另一个系统、获

取文件和关闭系统等。恶意事件包括对系统的破坏、在某个网络内 IP 包的泛滥、未经授权的情况下使用另一个用户的账户或系统的特殊权限、黑掉了一个或若干个网页以及执行恶意代码并毁坏了数据等。其他有害事件还包括水、火、断电和过热而导致系统瘫痪等。

"事件响应"的意思是事件发生后采取的措施和行动。这些行动措施通常是阻止和减小事件带来的影响。行动可能来自于人也可能来自于计算机系统。

事件响应的处理过程如下:

它包括 6 个阶段,准备、检测、抑制、根除、恢复和跟踪(称为 PDCERF 方法)。

1. 准备阶段

第 1 个阶段是准备,即在事件真正发生前为事件响应做好准备。这一阶段极为重要,因为当今的安全事件大多数都是复杂且费时的,准备是必须的而不是一种奢侈。准备阶段具体措施如下:

- 基于威胁建立一组合理的防御/控制措施。
- 建立一组尽可能高效的事件处理程序。
- 获得处理问题必须的资源和人员。
- 建立一个支持事件响应活动的基础设施。

2. 检测阶段

就事件响应而言,检测和入侵检测并不是同义词。检测意味着弄清是否出现了恶意代码、文件和目录是否被篡改或者出现其他的特征;如果是的话,问题在哪里?影响范围有多大?入侵检测最常见的含义是在确定对系统的非授权访问和滥用中是否发生入侵行为。比如,病毒感染可以用病毒检测软件而不是入侵检测软件来发现。因此,检测包含的范围要比入侵检测宽广得多。

从操作的角度来讲,事件响应过程中所有的动作都依赖于检测。坦率地说,没有检测,就没有真正意义上的事件响应,检测触发了事件的响应。这一点大大提升了检测在其他 5 个阶段的相对重要性。

3. 抑制阶段

抑制的目的是限制攻击的范围,同时也就限制了潜在的损失和破坏。抑制相关的活动当然只有在第 2 阶段观察到事件的确已经发生的基础上才能进行。

抑制阶段一个关键的部分是决策(也就是决定做什么,才能减小损失或破坏的范围)。决策包括下列一些措施。

- 完全关闭所有系统。
- 断开外部网络。这样至少允许本地用户获得一定的服务。
- 修改所有防火墙和路由器的过滤规则,拒绝来自发起攻击主机的所有的流量。
- 封锁或删除被攻破的登录账号。
- 提高系统或网络行为的监控级别。
- 设置诱饵服务器作为陷阱,"陷阱及伪装手段"。

- 关闭服务,比如文件传输服务,如果服务中的漏洞被利用的话。
- 反击攻击者的系统,一般来说应该避免这样做,而且在得到上级管理层明确的同意之前,一定不要这样做。

4. 根除阶段

在事件被抑制以后,找出事件根源并彻底将其根除。

软件对根除工作是很有帮助的,比如,防病毒软件可以消灭大多数感染系统的病毒,如果有在抑制阶段就应该消除的特洛伊木马程序(其他后门程序或其他使得事件传播的因素)此时还驻留在系统中,就该将其彻底清除。若用户的系统被极其危险的恶意病毒感染,清除病毒并重新格式化所有包含感染文件硬盘是最佳的选择。

5. 恢复阶段

PDCERF 事件响应方法学的第 5 个阶段是恢复。在事件的根源根除以后,恢复阶段定义下一阶段的行动。恢复的目标是把所有被攻破的系统和网络设备彻底地还原到它们正常的任务状态。

恢复时,从确保完好的介质上执行一次完整的系统恢复。这种策略能提供高度的可靠性,保证系统和网络部件确实回到他们正常的操作状态。注意,如果攻击者获得了超级用户的访问权,一次完整的恢复应该强制性地修改所有的口令。

数据恢复应该十分小心。一种较为安全的方法是从最新的完全备份中恢复数据,另一种方法是从容错系统硬件(如冗余磁盘阵列 RAID)中恢复镜像的数据。当然,必须保证这些文件和数据没有被破坏。

6. 跟踪阶段

PDCERF 方法学的最后一个阶段是跟踪,其整体目标是回顾并整合发生事件的相关信息。不幸的是,跟踪是最有可能被忽略的阶段(部分原因是资源有限而且事件处理人员在事件恢复后已经筋疲力尽)。然而,这一阶段也是非常关键的,如果这一步被忽略,很难预想事件响应工作的成功率有多大。

追踪网络攻击有多种不同的意思,这取决于这个术语的使用场合。狭义上来说,就是找到事件发生的源头。在大多数情况下是指发现 IP 地址、MAC 地址或认证的主机名。在另一方面来说它是指确定攻击者的身份。

追踪漏洞扫描是一个比较特殊的问题。在大部分网络环境下,漏洞扫描是经常发生的事情。现实中,追踪扫描和追踪入侵前兆是不同类型的事件。称为攻击追踪可能更好一些,但也许扫描追踪是最合适的称呼。但关键的是追踪扫描源是一件极不具效率的事情,因为大量的扫描是来自合法的被攻陷的主机。而且每天如此大量的扫描使得用户无法去追踪源头。因此这件事变得非常的不现实。虽然必须注意扫描这个问题,但在大多数情况下如果去追踪源头就太浪费时间和资源了。

9.3.3 IDS入侵特征库创建和解析

IDS要有效地捕捉入侵行为，必须拥有一个强大的入侵特征数据库，这就如同公安部门必须拥有健全的罪犯信息库一样。但是，IDS一般所带的特征数据库都比较死板，遇到“变脸”的入侵行为往往相逢不相识。因此，管理员有必要学会如何创建满足实际需要的特征数据样板，做到以不变应万变，在这里，将对入侵特征的概念、种类以及如何创建特征进行介绍，以帮助读者掌握对付入侵者“变脸”的方法。

1. 特征（signature）的基本概念

IDS中的特征就是指用于判别通信信息种类的样板数据，通常分为多种，以下是一些典型识别方法。

- 来自保留IP地址的连接企图。可通过检查IP报头（IP header）的来源地址轻易地识别。
- 带有非法TCP标志联合物的数据包。可通过对比TCP报头中的标志集与已知正确和错误标记联合物的不同点来识别。
- 含有特殊病毒信息的E-mail。可通过对比每封E-mail的主题信息和病态E-mail的主题信息来识别，或者通过搜索相似的特定名字来识别。
- 查询负载中的DNS缓冲区溢出企图。可通过解析DNS域及检查每个域的长度来识别利用DNS域的缓冲区溢出企图。还有另外一个识别方法是，在负载中搜索“壳代码利用”（exploit shellcode）的序列代码组合。
- 通过对POP3服务器发出成百上千次同一命令而导致的DoS攻击。通过跟踪记录某个命令连续发出的次数，看看是否超过了预设上限，而发出报警信息。
- 未登录情况下使用文件和目录命令对FTP服务器的文件访问攻击。通过创建具备状态跟踪的特征样板以监视成功登录的FTP对话、发现未经验证却发登录命令的入侵企图。

从以上分析可以看出特征的涵盖范围很广，有简单的报头域数值、有高度复杂的连接状态跟踪、有扩展的协议分析。一叶即可知秋，本小节将从最简单的特征入手，详细讨论其功能及开发、定制方法。

值得注意的是，不同的IDS产品具有的特征功能也有所差异。例如，有些网络IDS系统只允许少量地定制存在的特征数据或者编写需要的特征数据，而一些网络则允许在大范围内定制或编写特征数据，甚至可以是任意一个特征；一些IDS系统只能检查确定的报头或负载数值，另外一些则可以获取任何信息包的任何位置的数据。

2. 特征库的方式

特征是检测数据包中的可疑内容是否真正“不可用”的样板，也就是“破坏分子”的克隆。特征的定制或编写程度可粗可细，完全取决于实际需求。或者只是判断是否发生了异常行为而不确定具体是什么攻击行为，从而节省资源和时间；或者是判断出具体的攻击手段或漏洞利用方式，从而获取更多的信息。

3. 报头值

报头值(header values)的结构比较简单,而且可以很清楚地识别出异常报头信息,因此,特征数据的首席候选值就是报头值。一个经典的例子是,明显违背 RFC793 中规定的 TCP 标准、设置了 SYN 和 FIN 标记的 TCP 数据包。这种数据包被许多入侵软件采用,向防火墙、路由器以及 IDS 系统发起攻击。

非法报头值是特征数据的一个非常基础的部分,合法但可疑的报头值也同等重要。例如,如果存在到端口 31337 或 27374 的可疑连接,就完全有理由怀疑有特洛伊木马在活动;再附加上其他探测信息,就能够进一步地判断是“真马”还是“假马”。

4. 确定特征“候选人”

为了更好地理解如何开发基于报头值的特殊数据,下面通过分析一个实例,对整个过程进行详细阐述。

Synscan 是一个流行的用于扫描和探测系统的工具,由于它的代码被用于创建蠕虫 Ramen 的开始片断而在 2001 年早期大出风头。Synscan 的执行行为很具典型性,它发出的信息包具有多种可分辨的特性,包括如下特性。

- 不同的来源 IP 地址信息。
- TCP 来源端口 21,目标端口 21。
- 服务类型 0。
- IP 鉴定号码 39426(IP identification number)。
- 设置 SYN 和 FIN 标志位。
- 不同的序列号集合(sequence numbers set)。
- 不同的确认号码集合(acknowledgment numbers set)。
- TCP 窗口尺寸 1028 。

通过对以上数据进行筛选,看看哪个比较合适做特征数据。需要寻找的是非法、异常或可疑数据,大多数情况下,这都反映出攻击者利用的漏洞或者他们使用的特殊技术。以下是特征数据的候选对象。

- 只具有 SYN 和 FIN 标志集的数据包,这是公认的恶意行为迹象。
- 没有设置 ACK 标志,但却具有不同确认号码数值的数据包,而正常情况应该是 0。
- 来源端口和目标端口都被设置为 21 的数据包,经常与 FTP 服务器关联。这种端口相同的情况一般被称为“反身”(reflexive),除了个别时候进行一些特别 NetBIOS 通信外,正常情况下不应该出现这种现象。“反身”端口本身并不违反 TCP 标准,但大多数情况下它们并非预期数值。例如在一个正常的 FTP 对话中,目标端口一般是 21,而来源端口通常都高于 1023。
- TCP 窗口尺寸为 1028,IP 鉴定号码在所有数据包中为 39 426。根据 IP RFC 的定义,这 2 类数值应在数据包间有所不同,因此,如果持续不变,就表明可疑。

5. 选择最佳特征

从以上 4 个候选对象中，可以单独选出一项作为基于报头的特征数据，也可以选出多项组合作为特征数据。

选择一项数据作为特征有很大的局限性。例如，一个简单的特征可以是只具有 SYN 和 FIN 标志的数据包，虽然这可以很好地提示用户可能有一个可疑的行为发生，但却不能给出为什么会发生的更多信息。SYN 和 FIN 通常联合在一起攻击防火墙和其他设备，只要有它们出现，就预示着扫描正在发生、信息正在收集、攻击将要开始。

选择以上 4 项数据联合作为特征也不现实，因为这显得有些太特殊了。尽管能够精确地提供行为信息，但是比仅仅使用一个数据作为特征而言，会显得远远缺乏效率。实际上，特征定义永远要在效率和精确度间取得折中。大多数情况下，简单特征比复杂特征更倾向于误报(false positives)；复杂特征比简单特征更倾向于漏报(false negatives)。

由此看来，选择最佳特征是没有固定标准的，完全应由实际情况决定。例如，如果想判断攻击可能采用的工具是什么，那么除了 SYN 和 FIN 标志以外，还需要其他什么属性？“反身”端口虽然可疑，但是许多工具都使用到它，而且一些正常通信也有此现象，因此不适宜选为特征。TCP 窗口尺寸 1028 尽管有一点可疑，但也会自然的发生。IP 鉴定号码 39426 也一样。没有 ACK 标志的 ACK 数值很明显是非法的，因此非常适于选为特征数据。当然，根据环境的不同，及时地调整或组合特征数据，才能达到最优效果。

6. 一个特征库的建立

下面，创建一个特征库，用于检测由 Synscan 发出的每个 TCP 信息包，特征如下：

- 只设置了 SYN 和 FIN 标志。
- IP 鉴定号码为 39 426。
- TCP 窗口尺寸为 1028。

第一个项目太普遍，第二个和第三个项目联合出现在同一数据包的情况不是很多，因此，将这三个项目组合起来就可以定义一个详细的特征了。再加上其他的 Synscan 属性不会显著地提高特征的精确度，只能增加资源的耗费。

习　题　9

1. 入侵检测系统可分为哪几类？
2. 试述防火墙和入侵检测系统的基本功能及其应用范围。
3. 试述入侵检测系统的组成，并画出其工作流程图。
4. 网络入侵基本的检测方法有哪些？
5. 常用的入侵检测技术有哪些？
6. 试述异常检测模型和误用检测模型的基本功能，并对两者之间的区别进行分析。

第 10 章 chapter 10

端口扫描技术

10.1 端口扫描原理

10.1.1 端口的概念

1. 什么是端口

在计算机系统中,端口(port)泛指 I/O 端口,即“硬件端口”,也就是计算机的物理端口,如计算机的串口、并口、输入/输出设备端口、USB 接口以及适配器接口、网络连接设备集线器、交换机和路由器的连接端口等,这些端口都是可见的硬件接口。

在计算机网络通信技术中,端口不是物理意义上的端口,而是特指 TCP/IP 协议中的端口,是逻辑意义上的端口,TCP/IP 协议中端口分为两大类,面向连接服务的“TCP 端口”和无连接服务的“UDP 端口”。在本章中,主要介绍 TCP 端口。

TCP/UDP 端口指的是什么呢? 如果把计算机网络比作一间大屋子,那么端口就是出入这间屋子的“通道”,或说成是出入这间屋子的“大门”。换句话说,端口是用户与计算机网络的接口,人们是通过端口与网络打交道的。这里指的端口是看不见的“软件端口”。在本书中,所涉及的端口泛指的是这种“软件端口”。

在日常生活中,“门”上都有“门牌号”作为标记,而 TCP 端口是通过端口号来标记的。

端口是一组号码,占 16 个二进制位,其范围为 0～65 535,服务器在预设置端口等待客户端的连接。例如,WWW 服务使用 TCP 的 80 号端口,FTP 使用 21 号端口,Telnet 的端口号为 23 等。

端口定义了 TCP/UDP 和上层应用程序之间的接口点。客户程序可任意选择端口号,服务程序则使用固定的标准端口号,IP 地址和端口号的组合成为套接字 Socket,在一个主机上是唯一的。一条连接由客户端和服务器的套接字组成。

例如,在图 10-1 中有 3 个用户通过 Telnet 登录到服务器 C 上,一共有 3 个连接,表示为:

(202.112.97.82,500)与(202.112.97.94,23)连接

(202.112.97.82,501)与(202.112.97.94,23)连接

(202.112.97.84,500)与(202.112.97.94,23)连接

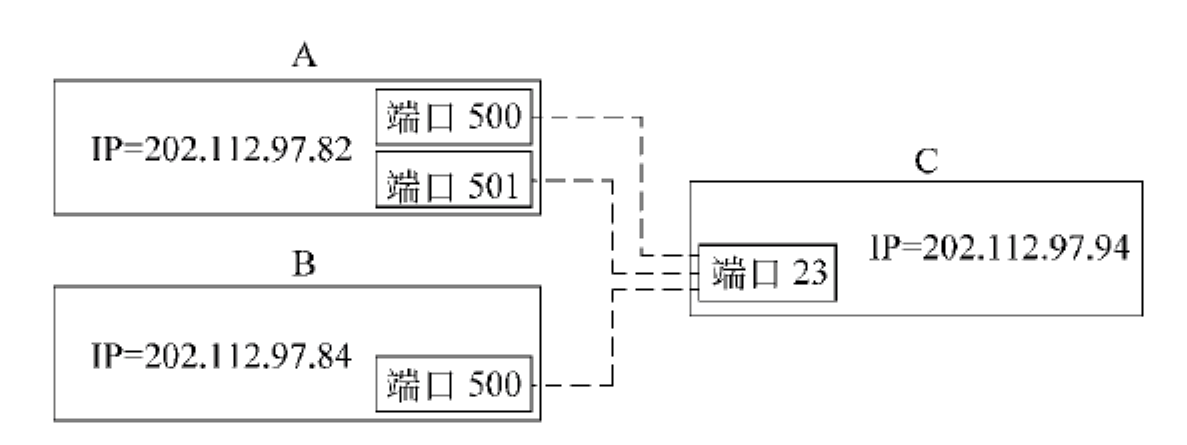


图 10-1　TCP 端口连接

对攻击者来讲,每一个端口就是一个入侵通道。对目标计算机进行端口扫描,能得到许多有用的信息,从而发现系统的安全漏洞。在 TCP/IP 网络协议中,各种服务提供的服务端口,网上的服务器及终端计算机都是通过端口进行通信和提供服务的。在计算机网络中,每个特定的服务都在一个特定的端口侦听,当用户有信息到达时,终端计算机就会检查数据包中的端口号,在这个特定的端口侦听的服务就是接收数据。常用的 TCP 端口如表 10-1 所示。

表 10-1　常用 TCP 端口分配表

序　号	端 口 号	协　　议	序　号	端 口 号	协　　议
1	13	Daytime(日期时间协议)	8	53	Domin(域)
2	20	FTP 数据连接	9	69	平凡文件传输协议 FFTP
3	21	FTP 控制连接	10	79	Finger 协议
4	23	TELNET 协议	11	80	WWW 协议
5	25	SMTP 协议	12	110	POP 协议
6	37	时间协议	13	139	NetBIOS 协议
7	43	Whois(信息查询协议)	14	3389	Windows 2000 超级终端协议

2. 端口的分类

按端口号分布划分,可分为周知端口和动态端口。

1) 周知端口(well known ports)

顾名思义,“周知端口”是众所周知的端口,也就是常用的端口,端口号在 0～1023 之间。周知端口通常是相对固定的端口,例如 80 端口分配给 WWW 服务,21 端口分配给 FTP 服务等。在 IE 的地址栏里输入一个网址的时候(比如 www.cce.com.cn)是不必指定端口号的,因为在默认情况下 WWW 服务的端口号是 80。TCP/UDP 端口分配详细情况请参见 http://www.iana.org 网站的 Most Popular Links 项下的 TCP and UDP Port Numbers。

网络服务是可以使用其他端口号的,如果不是默认的端口号则应该在地址栏上指定端口号,方法是在地址后面加上冒号“:”,再加上端口号。比如使用 8080 作为 WWW 服

务的端口，则需要在地址栏里输入 www.cce.com.cn:8080。

但是有些系统协议使用固定的端口号，它是不能被改变的，比如 139 端口专门用于 NetBIOS 与 TCP/IP 之间的通信，不能手动改变。

2）动态端口（dynamic ports）

动态端口的范围是 1024～65 535。之所以称为动态端口，是因为它一般不固定分配某种服务，而是动态分配。动态分配是指当一个系统进程或应用程序进程需要网络通信时，它向主机申请一个端口，主机从可用的端口号中分配一个供其使用。当这个进程关闭时，同时也就释放了所占用的端口号。

动态端口也常常被病毒木马程序所利用，而且有一定的对应关系，如冰河木马默认连接端口是 7626、WAY 2.4 病毒连接的端口是 8011、Netspy 3.0 连接的端口是 7306、YAI 病毒连接的端口是 1024 等。

按协议类型划分，可以分为 TCP、UDP、IP 和 ICMP 等端口。在本章中介绍的端口是 TCP 和 UDP 端口。

1）TCP 端口

TCP 端口，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。常见的包括 FTP 服务的 21 端口，Telnet 服务的 23 端口，SMTP 服务的 25 端口以及 HTTP 服务的 80 端口等。

2）UDP 端口

UDP 端口，即用户数据包协议端口，无需在客户端和服务器之间建立连接，其安全性得不到保障。常见的有 DNS 服务的 53 端口，SNMP 服务的 161 端口以及 QQ 使用的 8000 和 4000 端口等。

3. 常见端口服务功能

1）端口：0

服务：Reserved

说明：通常用于分析操作系统。这一方法能够工作是因为在一些系统中 0 是无效端口，当试图使用通常的闭合端口连接它时将产生不同的结果。一种典型的扫描是使用 IP 地址为 0.0.0.0，设置 ACK 位并在以太网层广播。

2）端口：1

服务：tcpmux

说明：这显示有人在寻找 SGI Irix 机器。Irix 是实现 tcpmux 的主要提供者，默认情况下 tcpmux 在这种系统中被打开。Irix 机器在发布时含有几个默认的无密码的账户，如 IP、GUEST UUCP、NUUCP、DEMOS 、TUTOR、DIAG 和 OUTOFBOX 等。许多管理员在安装后忘记删除这些账户，因此黑客可在 Internet 上搜索 tcpmux 并利用这些账户。

3）端口：7

服务：Echo

说明：能查看到许多人搜索 Fraggle 放大器时，发送到 X.X.X.0 和 X.X.X.255 的

信息。

4）端口：19

服务：Character Generator

说明：这是一种仅仅发送字符的服务。UDP 版本将会在收到 UDP 包后回应含有垃圾字符的包。TCP 连接时会发送含有垃圾字符的数据流直到连接关闭。黑客利用 IP 欺骗可以发动 DoS 攻击。伪造两个 chargen 服务器之间的 UDP 包。同样 Fraggle DoS 攻击向目标地址的这个端口广播一个带有伪造受害者 IP 的数据包，受害者为了回应这些数据而使网络过载。

5）端口：21

服务：FTP

说明：FTP 服务器所开放的端口，用于上传、下载文件。最常见的攻击者用于寻找打开 anonymous 的 FTP 服务器的方法。这些服务器带有可读写的目录。木马 Doly Trojan、Fore、Invisible FTP、WebEx、WinCrash 和 Blade Runner 都会开放这一端口。

6）端口：22

服务：ssh

说明：PcAnywhere 建立的 TCP 和这一端口的连接可能是为了寻找 ssh。这一服务有许多弱点，如果配置成特定的模式，许多使用 RSAREF 库的版本就会有不少的漏洞存在。

7）端口：23

服务：Telnet

说明：远程登录，入侵者在搜索远程登录 UNIX 的服务。大多数情况下扫描这一端口是为了找到机器运行的操作系统。木马 Tiny Telnet Server 开放端口就是 23。

8）端口：25

服务：SMTP

说明：SMTP 服务器所开放的端口，用于发送邮件。入侵者寻找 SMTP 服务器是为了传递 SPAM（垃圾邮件）。木马 Antigen、E-mail Password Sender、Haebu Coceda、Shtrilitz Stealth、WinPC 和 WinSpy 开放的都是这个端口。

9）端口：31

服务：MSG Authentication

说明：木马 Master Paradise、黑客 Paradise 开放此端口。

10）端口：42

服务：WINS Replication

说明：WINS 复制。

11）端口：53

服务：Domain Name Server（DNS）

说明：DNS 服务器所开放的端口，入侵者可能是试图进行区域传递（TCP），欺骗 DNS（UDP）或隐藏其他的通信，因此防火墙常常过滤或记录此端口。

12）端口：67

服务：Bootstrap Protocol Server

说明：通过 DSL 和 Cable modem 的防火墙常会看见大量发送到广播地址 255.255.255.255 的数据。这些机器在向 DHCP 服务器请求一个地址。黑客经常进入它们，分配一个地址把自己作为局部路由器而发起大量中间人(man-in-middle)攻击。客户端向 68 端口广播请求配置，服务器向 67 端口广播回应请求。

13）端口：69

服务：Trival File Transfer

说明：许多服务器与 bootp 一起提供这项服务，便于从系统下载启动代码。常常由于错误配置而使入侵者能从系统中窃取任何文件。

14）端口：79

服务：Finger Server

说明：入侵者用于获得用户信息，查询操作系统，探测已知的缓冲区溢出错误，回应从自己机器到其他机器 Finger 扫描。

15）端口：80

服务：HTTP

说明：用于网页浏览。木马 Executor 开放此端口。

16）端口：99

服务：Metagram Relay

说明：后门程序 ncx99 开放此端口。

17）端口：102

服务：Message transfer agent(MTA)-X.400 over TCP/IP

说明：消息传输代理。

10.1.2 端口扫描原理

端口有两种：UDP 端口和 TCP 端口。由于 UDP 端口是面向无连接的，从原理的角度来看，没有被扫描的可能，或者说不存在一种迅速而又通用的扫描算法；而 TCP 端口具有连接定向(connection oriented)的特性(即是有面向连接的协议)，为端口的扫描奠定了基础，所以，本章介绍的端口扫描技术，是基于 TCP 端口的。TCP 建立连接时有 3 次握手，首先，Client 端往 Server 某一端口发送请求连接的 SYN 包，如果 Server 的这一端口允许连接，就会给 Client 端发一个 ACK 回包，Client 端收到 Server 的 ACK 包后再给 Server 端发一个 ACK 包，TCP 连接正式建立，这就是连接成功的过程，如图 10-2 所示。

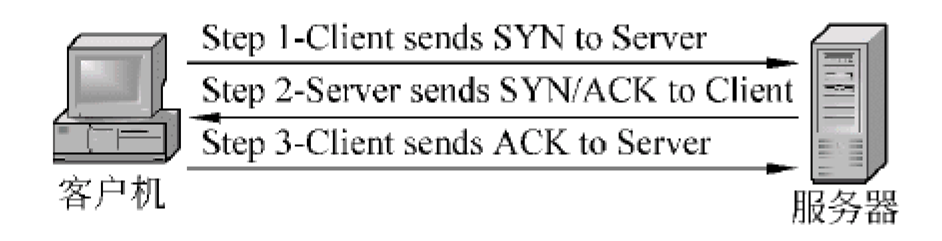


图 10-2 TCP 连接成功的响应过程

当 Client 端往 Server 某一端口发送请求连接的 SYN 包，此时若 Server 的这一端口不允许连接，就会给 Client 端发一个 RST 回包，Client 端收到 Server 的 RST 包后再给 Server 端发一个 RST 包，这就是连接失败的过程，如图 10-3 所示。基于连接的建立过程，可以想到，假如要扫描某一个 TCP 端口，可以往该端口发一个 SYN 包，如果该端口处于打开状态，就可以收到一个 ACK。也就是说，如果收到 ACK，就可以判断目标端口处于打开状态，否则，目标端口处于关闭状态。这就是 TCP 端口扫描的基本原理。

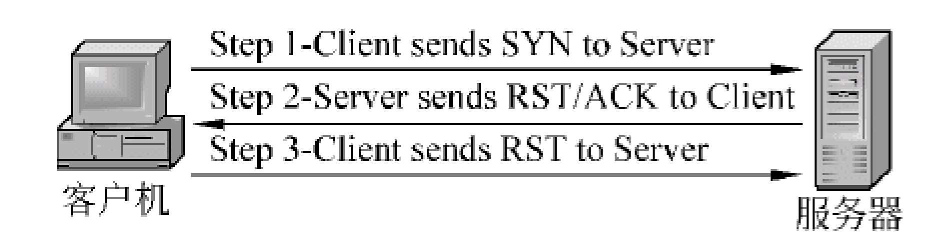


图 10-3　TCP 连接失败的响应过程

“端口扫描”通常指对目标计算机的所有需要扫描的端口发送同一信息，然后根据返回端口状态来分析目标计算机的端口是否打开、是否可用。“端口扫描”行为的一个重要特征是，在短时期内有很多来自相同的信源地址传向不同的目的地端口的包。

对于用端口扫描进行攻击的人来说，攻击者总是可以做到在获得扫描结果的同时，使自己很难被发现或者说很难被逆向跟踪。为了隐藏攻击，攻击者可以慢慢地进行扫描。通常来说，用长时间间隔的端口扫描是很难被识别的。隐藏源地址的方法是发送大量的(数千个或上万个)欺骗性的端口扫描包，其中只有一个包的源地址是真实的。这样，即使全部包都被拦截并被记录下来，要想辨别哪一个是真正的信源地址也是很困难的，因为只有一个包的源地址是真实的。

通常进行端口扫描的工具主要采用的是端口扫描软件，也通称之为“端口扫描器”，端口扫描可以提供以下 3 个用途：

- 识别目标系统上正在运行的 TCP 协议和 UDP 协议服务。
- 识别目标系统的操作系统类型(Windows 2000/XP、Windows NT 或 UNIX 等)。
- 识别某个应用程序或某个特定服务的版本号。

端口扫描器是一种自动检测远程或本地计算机安全性弱点的程序，甚至使用扫描器可不留痕迹的发现远程服务器的各种 TCP 协议端口的分配及提供的服务，可以得知它们所使用的软件版本，这就能间接地了解到远程计算机所存在的安全缺陷。

端口扫描器通过选用远程 TCP/IP 协议不同端口的服务，记录目标计算机端口给予的应答方法，可以搜集到很多关于目标计算机的信息。比如，是否有端口在侦听，是否允许匿名登录，是否有可写的 FTP 目录，是否能用 Telnet 等。

端口扫描器并不是一个直接攻击网络漏洞的程序，它仅仅能帮助发现目标机的某些内在的弱点。一个好的扫描器还能对它得到的数据进行分析，帮助查找目标计算机的漏洞。

端口扫描器在扫描过程中主要具有以下 3 个方面的能力：

- 发现一个计算机或网络的能力。
- 一旦发现一台计算机，就可发现目标计算机正在运行什么服务的能力。
- 通过测试目标计算机上的这些服务，发现存在的漏洞的能力。

编写扫描器程序必须要具有很多 TCP/IP 协议程序编写、C、Perl 或 SHELL 语言的

知识，需要一些 Socket 编程的背景，还需一种在开发客户/服务应用程序的方法。

10.1.3 常用端口和漏洞扫描技术

端口扫描就是得到目标主机开放和关闭的端口列表，这些开放的端口往往与一定的服务相对应，通过这些开放的端口，就能了解主机运行的服务，然后就可以进一步整理和分析这些服务可能存在的漏洞，随后采取针对性的攻击。

1. TCP connect 扫描

这是最基本的扫描方式。如果目标主机上的某个端口处于侦听状态，可根据其 IP 地址和端口号并调用 connect()与其建立连接。若目标主机未开放该端口，则 connect 操作失败。因此，使用这种方法可以检测到目标主机开放了哪些端口。注意，在执行这种扫描方式时，不需要对目标主机拥有任何权限。

2. TCP SYN 扫描

这种技术通常认为是“半”扫描，因为扫描程序不必与目标主机三次握手就可建立一个完全的 TCP 连接。扫描程序发送一个 SYN 数据包，等待目标主机的应答。如果目标主机返回 SYN|ACK，表示端口处于侦听状态。若返回 RST，表示端口没有处于侦听状态。如果收到一个 SYN|ACK，则扫描程序发送一个 RST 数据包，来终止这个连接。这种扫描技术的优点在于一般不会在目标计算机上留下痕迹。但要求攻击者在发起攻击的计算机上必须有 root 权限，因为不是通过 connect 调用来扫描端口，必须直接在网络上向目标主机发送 SYN 和 RST 数据包。

3. TCP FIN 扫描

一些防火墙和包过滤器会对一些指定的端口进行监视，因此 TCP SYN 扫描攻击可能会被检测并记录下来。FIN 数据包可以通过它们而不留痕迹。向目标主机的某个端口发送 FIN 数据包，若端口处于侦听状态，目标主机不会回复 FIN 数据包。相反，若端口未被侦听，目标主机会用适当的 RST 来回复。这种方法依赖于系统的实现。某些系统对所有的 FIN 一律回复 RST，而不管端口是否打开，在这种情况下，TCP FIN 扫描是不适用的。

4. IP 分片扫描

这种方法并不直接发送 TCP 探测数据包，而是预先将数据包分成两个较小的 IP 数据包传送给目标主机。目标主机收到这些 IP 包后，会把它们组合还原为原先的 TCP 探测数据包。将数据包分片的目的是使它们能够通过防火墙和包过滤器，将一个 TCP 分为几个较小的数据包，可能会穿过防火墙而到达目标主机。

5. TCP 反向 ident 扫描

ident 协议(RFC 1413)允许通过 TCP 连接列出任何进程拥有者的用户名(包含该进

程拥有何种权限)。因此,扫描器能连接到 http 端口,然后检查 httpd 是否正在以 root 权限运行。

6. FTP 反射攻击

FTP 协议的一个特性是支持代理(proxy)FTP 连接。即入侵者可以通过自己的计算机和目标主机的 FTP server-PI(协议解释器)连接,建立一个控制通信连接。然后,请求这个 server-PI 激活一个有效的 server_DTP(数据传输进程)来给 Internet 的任何地方发送文件。

7. UDP 端口扫描

这种方法与上面几种方法的不同之处在于使用 UDP 协议。由于 UDP 协议较 TCP 简单,所以要判断一个端口是否被侦听较为困难。这是由于处于侦听状态的端口对扫描探测并不发送确认,而未侦听的端口也并不会返回错误数据包。

8. UDP recvfrom()和 write()扫描

若在发起攻击的计算机上没有 root 权限,就不能得到端口不可达的 ICMP_PORT_UNREACH 错误数据包。在 Linux 中可以间接的检测到是否收到了目标主机的这个应答数据包。例如,对一个未侦听端口的第二个 write()调用将失败。在非阻塞的 UDP 套接字上调用 recvfrom()时,如果未收到这个应答,返回 EAGAIM(其意思是可以"重试")。如果收到这个应答,则返回 ECONNREFUSED(连接被拒绝)。可以根据 recvfrom()和 write()的返回信息来判断目标主机是否发送了 ICMP_PORT_UNREACH 应答。

9. ICMP_echo 扫描

通过执行 ping 命令,可以判断出在一个网络上主机是否能到达(即主机是否在线)。

10.2 常用扫描命令及扫描工具

10.2.1 常用扫描命令

1. ping 命令

ping 命令主要是用来对 TCP/IP 网络进行诊断,其原理是通过对目标计算机发送一个 IP 数据包,若目标计算机网络工作正常,则会将这个 IP 数据包返到发送端,如果返回的数据包与发送出去的数据完全一致,说明 ping 命令成功,否则说明 ping 失败。通过 ping 的结果可以判断目标计算机是否在线、网络工作是否正常,同时还能知道该数据包从发送到返回需要多少时间。

ping 命令的格式为:

ping<参数><hostname>

其中 hostname 为目标主机名(域名或 IP 地址)。

除此之外,ping 命令还可用来进行网络攻击。其攻击手段是通过该命令给目标计算机发送一个很大的数据包,目标计算机不得不忙于回应,从而大量地消耗目标计算机的资源。可用下面的命令进行攻击:

ping -l n <hostname>

命令中的参数 *n* 为发送数据包的长度(以字节为单位)。

由于这一条命令可以给目标计算机发送一个很大的数据包,目标计算机同样要接收并返回一个同样大的数据包,若有多台计算机同时向某一台目标计算机发送上述命令,则这台目标计算机就会因应付回包而喘不过气来,严重时会导致网络拒绝服务甚至瘫痪,这就达到了攻击的目的。

下面,分别用 ping 命令向 163. com 发送 50 个、5000 个和 50 000 个字节的数据包,其运行结果如图 10-4、图 10-5 和图 10-6 所示。

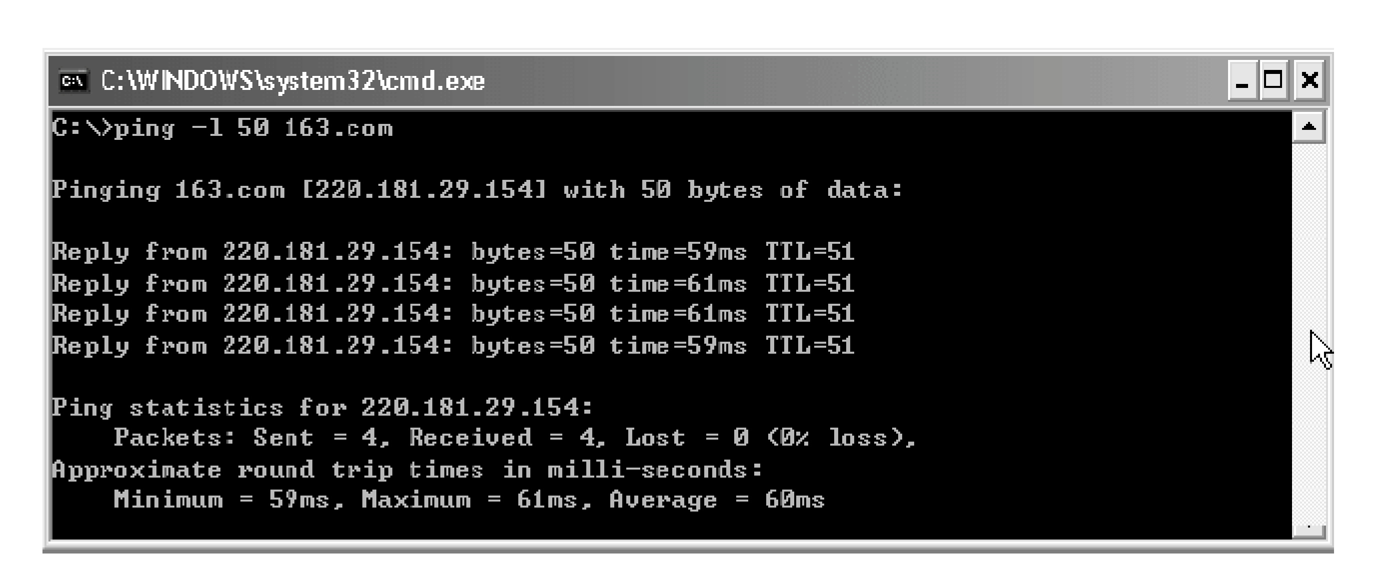


图 10-4 ping 50 个字节数据包的结果

```
C:\WINDOWS\system32\cmd.exe
C:\>ping -l 5000 163.com

Pinging 163.com [220.181.29.154] with 5000 bytes of data:

Reply from 220.181.29.154: bytes=5000 time=137ms TTL=51
Reply from 220.181.29.154: bytes=5000 time=136ms TTL=51
Reply from 220.181.29.154: bytes=5000 time=131ms TTL=51
Reply from 220.181.29.154: bytes=5000 time=131ms TTL=51

Ping statistics for 220.181.29.154:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 131ms, Maximum = 137ms, Average = 133ms

C:\>
```

图 10-5 ping 5000 个字节数据包的结果

从图 10-4 和图 10-5 可看出,用 ping 命令发送检测包时,发送 5000 个字节数据包返回的时延明显比发送 50 个字节数据包的时延长得多。若发送 50 000 个字节长的数据包,则会发生超时现象,如图 10-6 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\>
C:\>ping -l 50000 163.com

Pinging 163.com [220.181.29.154] with 50000 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 220.181.29.154:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
C:\>
C:\>
```

图 10-6　ping 超时

2. tracert 命令

tracert 命令用来跟踪一个数据包发送到目标计算机中间经过的路由，同时可得到每一个路由所需的时延。

例如，从主机 10.1.23.33 发出一条命令 tracert 163.com，得到如图 10-7 示的屏幕。

```
C:\WINDOWS\system32\cmd.exe
C:\>
C:\>tracert 163.com

Tracing route to 163.com [220.181.29.154]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.1.23.1
  2    <1 ms    <1 ms    <1 ms  172.16.0.199
  3    15 ms    19 ms    28 ms  202.101.72.1
  4     2 ms     2 ms     6 ms  61.189.177.73
  5     1 ms     3 ms     4 ms  61.189.177.149
  6     3 ms     1 ms     1 ms  202.97.17.49
  7     *       15 ms    15 ms  202.97.42.29
  8    57 ms    59 ms    58 ms  202.97.34.129
  9    57 ms    61 ms    59 ms  218.30.25.49
 10    57 ms    57 ms    57 ms  218.30.25.74
 11    70 ms    68 ms    72 ms  220.181.16.14
 12    68 ms    68 ms    63 ms  220.181.17.58
 13    57 ms    58 ms    57 ms  220.181.29.154

Trace complete.

C:\>_
```

图 10-7　tracert 命令扫描结果

tracert 会自动向目标主机发送 3 个不同的数据包，每一个路由设备都会将这 3 个数据包返回，所以每一个路由都会看到 3 个时延，如图 10-7 所示。图中时延为“＊”者表示超时。

3. Rusers 和 Finger

这两条都是 UNIX 命令。通过这两个命令，能收集到目标计算机上的有关用户的消息。

使用 Rusers 命令，产生的结果如下所示。

```
gajake snark.wizard.com: ttyp1 Nov 13 15: 42 7: 30 (remote)
root snark.wizard.com: ttyp2 Nov 13 14: 57 7: 21 (remote)
robo snark.wizard.com: ttyp3 Nov 15 01: 04 01 (remote)
angel111 snark.wizard.com: ttyp4 Nov14 23: 09 (remote)
pippen snark.wizard.com: ttyp6 Nov 14 15: 05 (remote)
root snark.wizard.com: ttyp5 Nov 13 16: 03 7: 52 (remote)
gajake snark.wizard.com: ttyp7 Nov 14 20: 20 2: 59 (remote)
dafr snark.wizard.com: ttyp15Nov 3 20: 09 4: 55 (remote)
dafr snark.wizard.com: ttyp1 Nov 14 06: 12 19: 12 (remote)
dafr snark.wizard.com: ttyp19Nov 14 06: 12 19: 02 (remote)
```

使用 Rusers 命令可以看到远程登录的用户名，并包括上次登录时间，使用的 SHELL 类型等信息。

使用 Finger 可以产生类似下面的结果。

```
user S00 PPP ppp-122-pm1.wiza Thu Nov 14 21: 29: 30 -still logged in
user S15 PPP ppp-119-pm1.wiza Thu Nov 14 22: 16: 35 -still logged in
user S04 PPP ppp-121-pm1.wiza Fri Nov 15 00: 03: 22 -still logged in
user S03 PPP ppp-112-pm1.wiza Thu Nov 14 22: 20: 23 -still logged in
user S26 PPP ppp-124-pm1.wiza Fri Nov 15 01: 26: 49 -still logged in
user S25 PPP ppp-102-pm1.wiza Thu Nov 14 23: 18: 00 -still logged in
user S17 PPP ppp-115-pm1.wiza Thu Nov 14 07: 45: 00 -still logged in
user S-1 0.0.0.0 Sat Aug 10 15: 50: 03 -still logged in
user S23 PPP ppp-103-pm1.wiza Fri Nov 15 00: 13: 53 -still logged in
user S12 PPP ppp-111-pm1.wiza Wed Nov 13 16: 58: 12 -still logged in
```

该命令能显示用户的状态。该命令是建立在客户/服务模型之上的。用户通过客户端软件向服务器请求信息，然后解释这些信息，提供给用户。在服务器上一般运行一个叫做 fingerd 的程序，根据服务器机器的配置，能向客户提供某些信息。如果考虑到保护这些个人信息的话，有可能许多服务器不提供这种服务，或者只提供一些无关的信息。

4. host 命令

host 是一个 UNIX 命令，它的功能和标准与 nslookup 查询一样。唯一的区别是 host 命令比较容易理解。host 命令的危险性相当大，下面举个使用实例，演示一次对 bu.edu 的 host 查询。

```
host -l -v -t any bu.edu
```

这条命令的执行结果所得到的信息非常多，包括操作系统、机器和网络的很多数据。基本信息如下：

```
Found 1 addresses for BU.EDU
Found 1 addresses for RS0.INTERNIC.NET
Found 1 addresses for SOFTWARE.BU.EDU
Found 5 addresses for RS.INTERNIC.NET
```

```
Found 1 addresses for NSEGC.BU.EDU
Trying 128.197.27.7
bu.edu 86400 IN SOA BU.EDU HOSTMASTER.BU.EDU(
961112121 ;serial (version)
900 ;refresh period
900 ;retry refresh this often
604800 ;expiration period
86400 ;minimum TTL)
bu.edu 86400 IN NS SOFTWARE.BU.EDU
bu.edu 86400 IN NS RS.INTERNIC.NET
bu.edu 86400 IN NS NSEGC.BU.EDU
bu.edu 86400 IN A 128.197.27.7
```

利用上述网络命令，可以收集到许多有用的信息，比如一个域里的名字服务器的地址，一台计算机上的用户名，一台服务器上正在运行什么服务，这个服务是哪个软件提供的，计算机上运行的是什么操作系统。

如果知道目标计算机上运行的操作系统和服务应用程序后，就能利用已经发现的漏洞来进行攻击。如果目标计算机的网络管理员没有对这些漏洞及时修补的话，入侵者能轻而易举地闯入该系统，获得管理员权限，并留下后门。

如果入侵者得到目标计算机上的用户名后，能使用口令破解软件，多次试图登录目标计算机。经过尝试后，就有可能进入目标计算机。得到了用户名，就等于得到了进入目标计算机的部分权限，剩下的只是使用软件进行攻击而已。

10.2.2 SuperScan

SuperScan 是由 Foundstone 开发的扫描软件工具，其功能十分强大，与许多同类工具比较，它既是一款网络安全工具，又是一款网络黑客攻击工具。黑客可以利用它进行拒绝服务攻击 DoS(Denial of Service)功能来收集远程网络主机信息。而作为安全工具，SuperScan 能够帮助用户发现网络中的脆弱点。

在这里，介绍的是 SuperScan SuperScan 4.0 版本，该软件是免费的，可以在如下地址 http://www.skycn.com/soft/8061.html 下载。

1. SuperScan 的启动

给 SuperScan 解压后，双击 SuperScan4.exe，开始启动。打开主界面，默认为扫描(Scan)菜单，允许输入一个或多个主机名或 IP 范围，也可以选文件下的输入地址列表。输入主机名或 IP 范围后开始扫描，单击左下角的▶按钮，SuperScan 开始扫描，如图 10-8 所示。

扫描进程结束后，SuperScan 将提供一个主机列表，显示每台扫描过的主机开放端口的信息。

在图 10-8 中，单击“查看 HTML 结果”按钮，可以以 HTML 格式显示有关信息，



图 10-8　SuperScan 主屏幕

如图 10-9 所示。

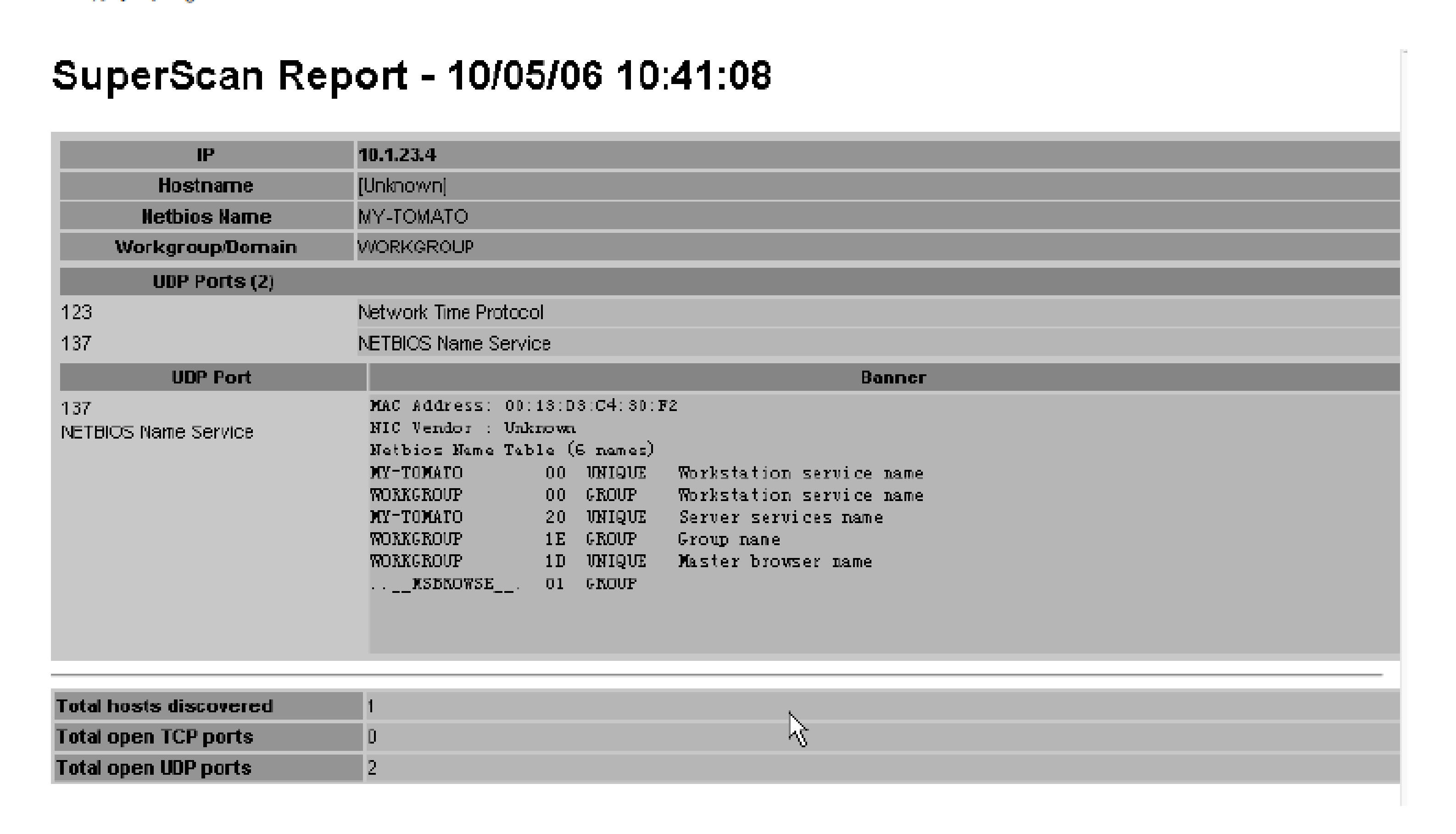


图 10-9　HTML 显示屏幕

在图 10-9 中，可以看到 SuperScan 扫描了哪些主机和在每台主机上哪些端口是开放的。

2. 主机和服务器扫描设置(host and service discovery)

经过上面的介绍，能够从一群主机中执行简单的扫描，然而，很多时候需要定制扫描。在图 10-8 中，选择“主机和服务器扫描设置”选项卡，可以定制扫描，如图 10-10 所示。



图 10-10　主机和服务扫描设置

3. 扫描选项(scan options)

“扫描选项”选项卡如图 10-11 所示，允许控制扫描进程。菜单中的首选项是定制扫描过程中主机和通过审查的服务数。



图 10-11　扫描选项

扫描选项中接下来的选项，能够设置主机名解析的次数。正常情况下，该次数设置1已足够了，除非用户的连接不可靠。

另一个选项是获取标志(banner grabbing)的设置，获取标志是根据显示一些信息尝试得到远程主机的回应。默认的延迟是8000毫秒，如果所连接的主机较慢，可以修改这个值。

旁边的滚动条是扫描速度调节选项，能够利用它来调节 SuperScan 在发送每个包所要等待的时间。最快扫描，是调节滚动条为0。可是，扫描速度设置为0，有包溢出的潜在可能。如果担心由于 SuperScan 引起的过量包溢出，最好调慢 SuperScan 的速度。

4. 工具(tools)选项

SuperScan 的工具选项(Tools)允许用户很快的得到许多主机信息。正确输入主机名或者 IP 地址和默认的连接服务器，然后单击要得到相关信息的按钮。例如，能 ping 一台服务器，或 traceroute，和发送一个 HTTP 请求。图 10-12 显示了得到的各种信息。



图 10-12 能够通过点选不同的按钮，收集各种主机信息

5. Windows 枚举选项(windows enumeration)

利用 Windows 枚举选项，可以查看 Windows 主机大量的枚举信息，如图 10-13 所示。



图 10-13　Windows 枚举选项

10.2.3　X-Scan

1. 软件功能

X-Scan 采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式，扫描内容包括远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞和拒绝服务漏洞等。对于多数已知漏洞，给出了相应的漏洞描述、解决方案及详细描述链接。

本小节介绍 X-Scan v3.3 简体中文版的使用技术。

2. 系统组成

X-Scan v3.3 简体中文版由下列文件组成。

xscan_gui.exe	X-Scan 图形界面主程序
checkhost.dat	插件调度主程序
update.exe	在线升级主程序
*.dll	主程序所需动态链接库
使用说明.txt	X-Scan 使用说明
/dat/language.ini	多语言配置文件,可通过设置"LANGUAGE\SELECTED"项进行语言切换
/dat/language.*	多语言数据文件
/dat/config.ini	当前配置文件,用于保存当前使用的所有设置
/dat/*.cfg	用户自定义配置文件
/dat/*.dic	用户名/密码字典文件,用于检测弱口令用户
/plugins	用于存放所有插件(后缀名为.xpn)
/scripts	用于存放所有 NASL 脚本(后缀名为.nasl)

/scripts/desc　　用于存放所有 NASL 脚本多语言描述(后缀名为.desc)
/scripts/cache　　用于缓存所有 NASL 脚本信息,以便加快扫描速度(该目录可删除)

3. 软件运行环境

Windows NT/2000/XP/2003。

4. 软件的启动

运行 X-Scan v3.3 简体中文版文件夹中的 scan_gui.exe 文件,即启动 X-Scan v3.3 简体中文版系统,如图 10-14 所示。



图 10-14　X-Scan v3.3 主屏幕

5. 扫描参数设置

选择"设置"|"扫描参数设置"命令,进入扫描参数设置屏幕,如图 10-15 所示。

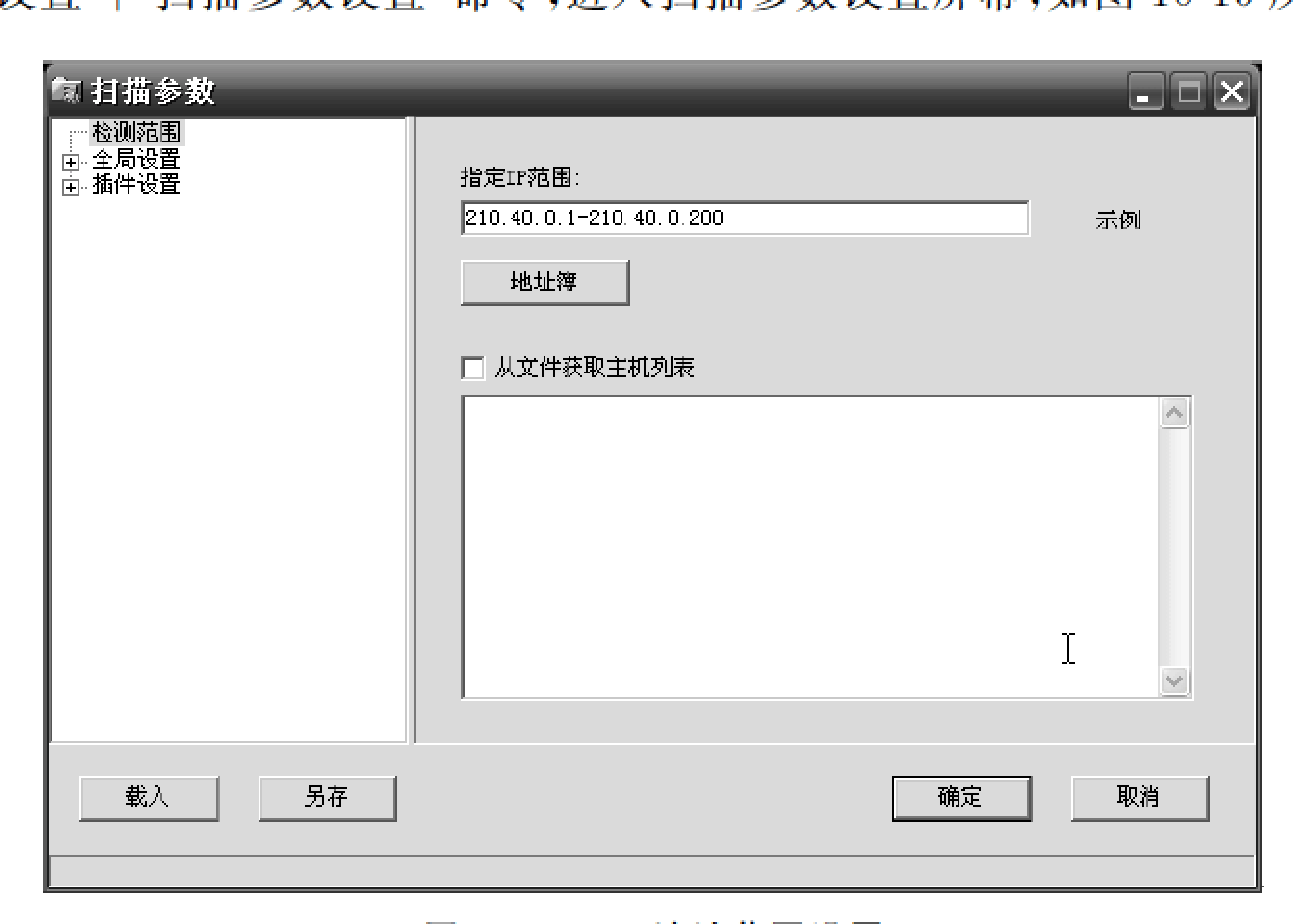


图 10-15　IP 地址范围设置

1）检测范围设置

在图 10-15 所示的屏幕进行设置。

①“指定 IP 范围”。可以输入独立 IP 地址或域名，也可输入以“-”和“，”分隔的 IP 范围，如 210.40.0.1-210.40.0.200 或类似 192.168.100.1/24 的掩码格式。

②“从文件中获取主机列表”。选中该复选框将从文件中读取待检测主机地址，文件格式应为纯文本，每一行可包含独立 IP 或域名，也可包含以“-”和“，”分隔的 IP 范围。

2）“全局设置”模块

在图 10-15 中，展开左上角的“全局设置”项，得到全局设置屏幕，如图 10-16 所示。



图 10-16　全局参数设置

(1)“扫描模块”项。用以选择本次扫描需要加载的插件，如图 10-16 所示。

(2)“并发扫描”项。用以设置并发扫描的主机和并发线程数，也可以单独为每个主机的各个插件设置最大线程数，如图 10-17 所示。



图 10-17　并发扫描设置

(3)“扫描报告”项。用以设置扫描结束后生成的报告文件名，保存在 LOG 目录下。扫描报告目前支持 TXT、HTML 和 XML3 种格式，如图 10-18 所示。

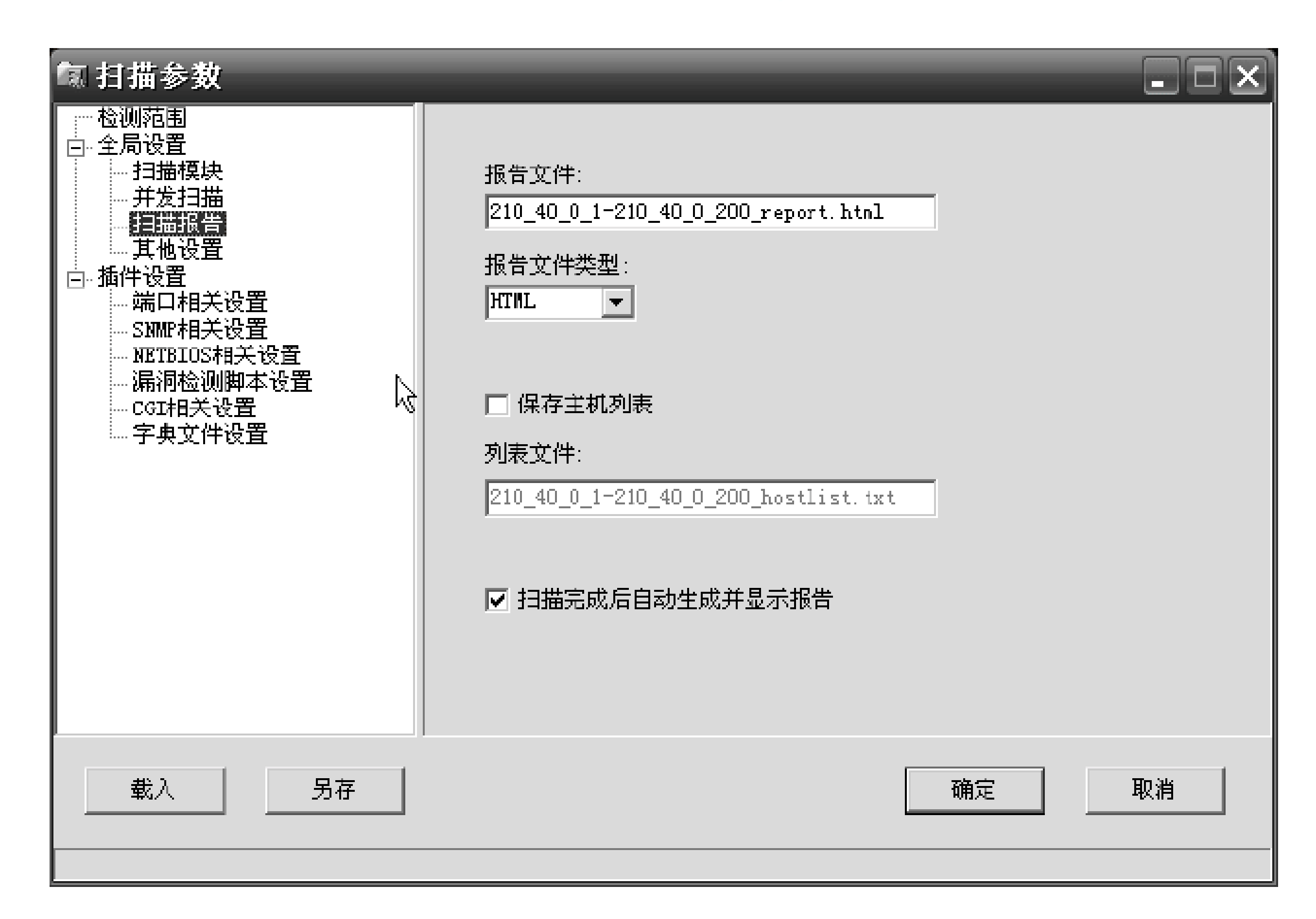


图 10-18　扫描报告文件设置

(4)“其他设置”项。用以设置其他一些参数，如图 10-19 所示。

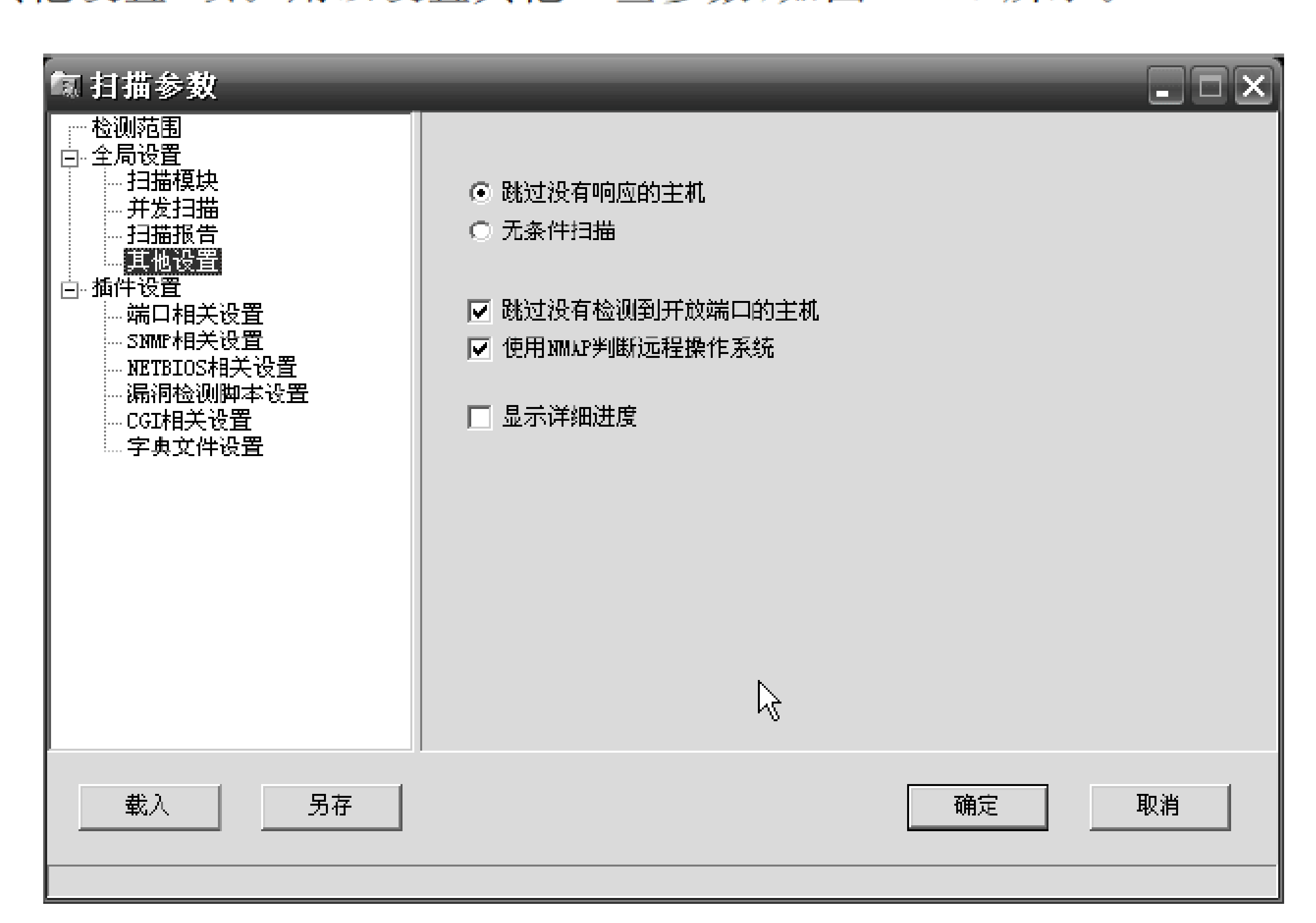


图 10-19　其他项设置

- “跳过没有响应的主机”。若目标主机不响应 ICMP ECHO 及 TCP SYN 报文，X-Scan 将跳过对该主机的检测。
- “无条件扫描”。对目标计算机无条件地扫描。
- “跳过没有检测到开放端口的主机”。若在用户指定的 TCP 端口范围内没有发现开放端口，将跳过对该主机的后续检测。
- “使用 NMAP 判断远程操作系统”。X-Scan 使用 SNMP、NETBIOS 和 NMAP 综

合判断远程操作系统类型，若 NMAP 频繁出错，可关闭该选项。

3）插件设置

在图 10-15 中，展开左上角的“插件设置”项，得到插件设置屏幕，如图 10-20 所示。

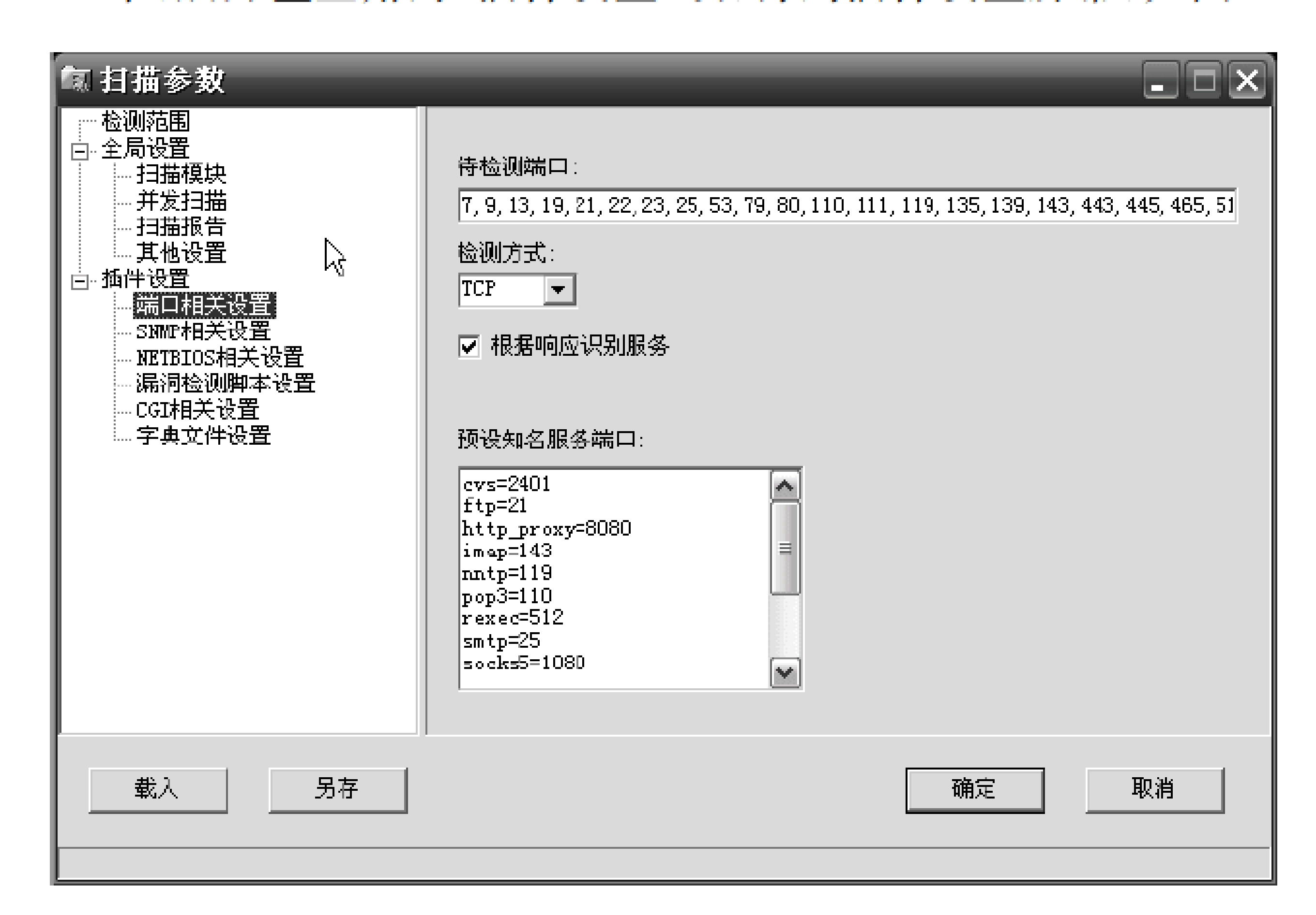


图 10-20 端口设置

（1）端口相关参数设置。用以设置扫描端口及其相关参数，如图 10-20 所示。

- “待检测端口”。输入以“-”和“,”分隔的 TCP 端口范围。
- “检测方式”。目前支持 TCP 完全连接和 SYN 半开扫描两种方式。
- “根据响应识别服务”。根据端口返回的信息智能判断该端口对应的服务。
- “预设知名服务端口”。用以预设各种常用服务的端口。

（2）SNMP 相关参数设置。用以设置 SNMP（简单网络管理协议）的相关参数，如图 10-21 所示。



图 10-21 SNMP 相关参数设置

(3) NETBIOS 相关参数设置。用以设置 NETBIOS 相关参数，如图 10-22 所示。

图 10-22　NETBIOS 相关参数设置

(4) 漏洞检测脚本参数设置。用以进行漏洞检测脚本设置，如图 10-23 所示。



图 10-23　漏洞检查脚本设置

(5) CGI 相关参数设置。用以设置 CGI 相关参数，如图 10-24 所示。

(6) 字典文件设置。用以设置各服务对应的密码字典文件。

6. 扫描

在图 10-14 所示的屏幕中，选择“文件”|“开始扫描”命令或单击快捷工具栏中的▶按钮，即开始扫描，如图 10-25 所示。

- “普通信息”。用以查看正在进行哪些项目的扫描，如图 10-26 所示。



图 10-24　CGI 相关参数设置

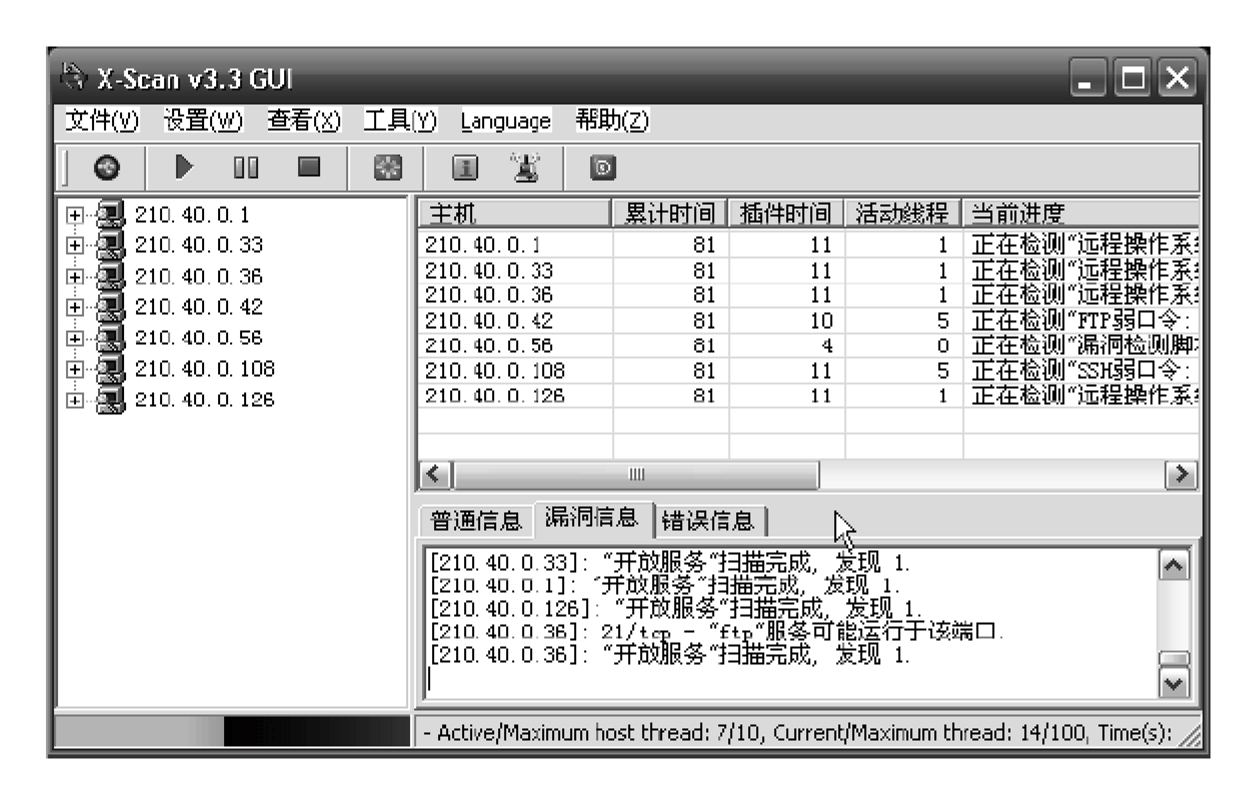


图 10-25　扫描过程

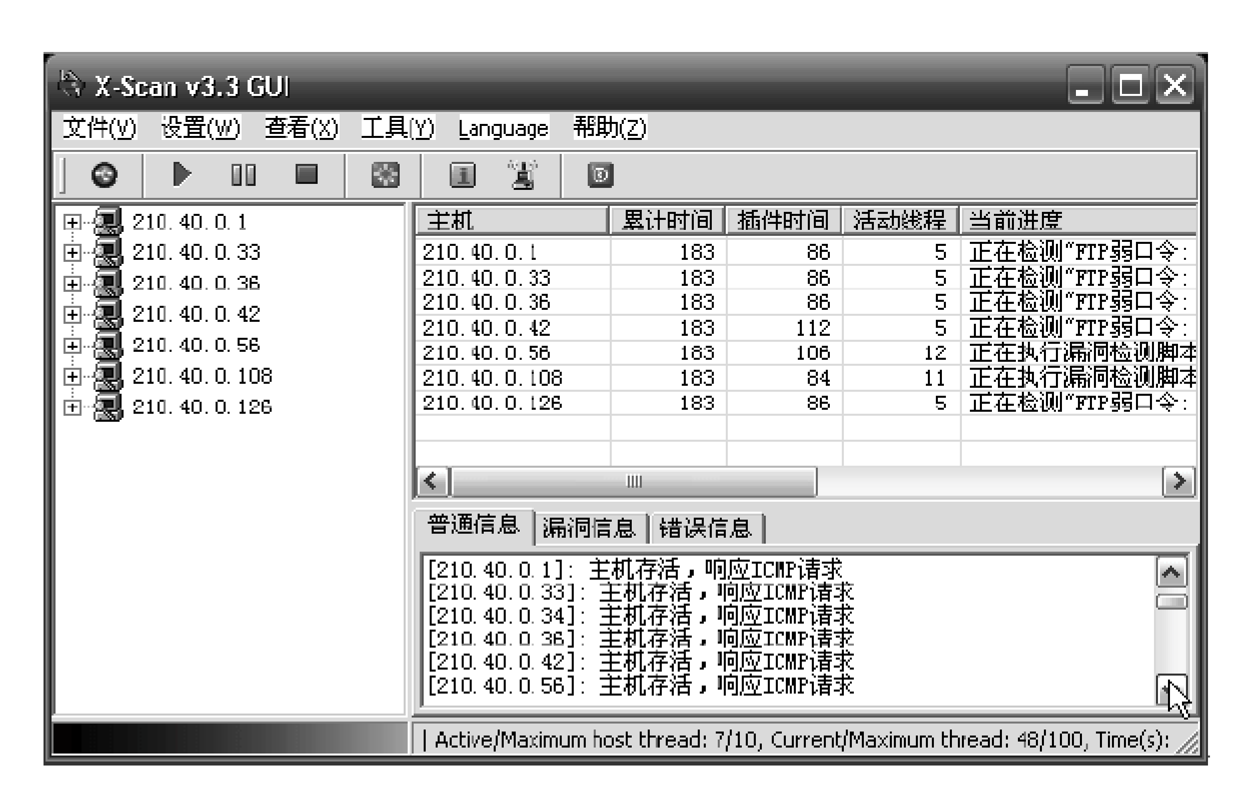


图 10-26　普通信息

• “漏洞信息”。用以查看目标计算机上存在的漏洞,如图 10-25 所示。
• “错误信息”。用以查看目标计算机上存在的错误。

7. 扫描报告

扫描结束后,系统会自动以 HTML 文件格式显示扫描结果报告,如图 10-27 所示。也可选择“查看”|“检测报告”命令查看检测报告。

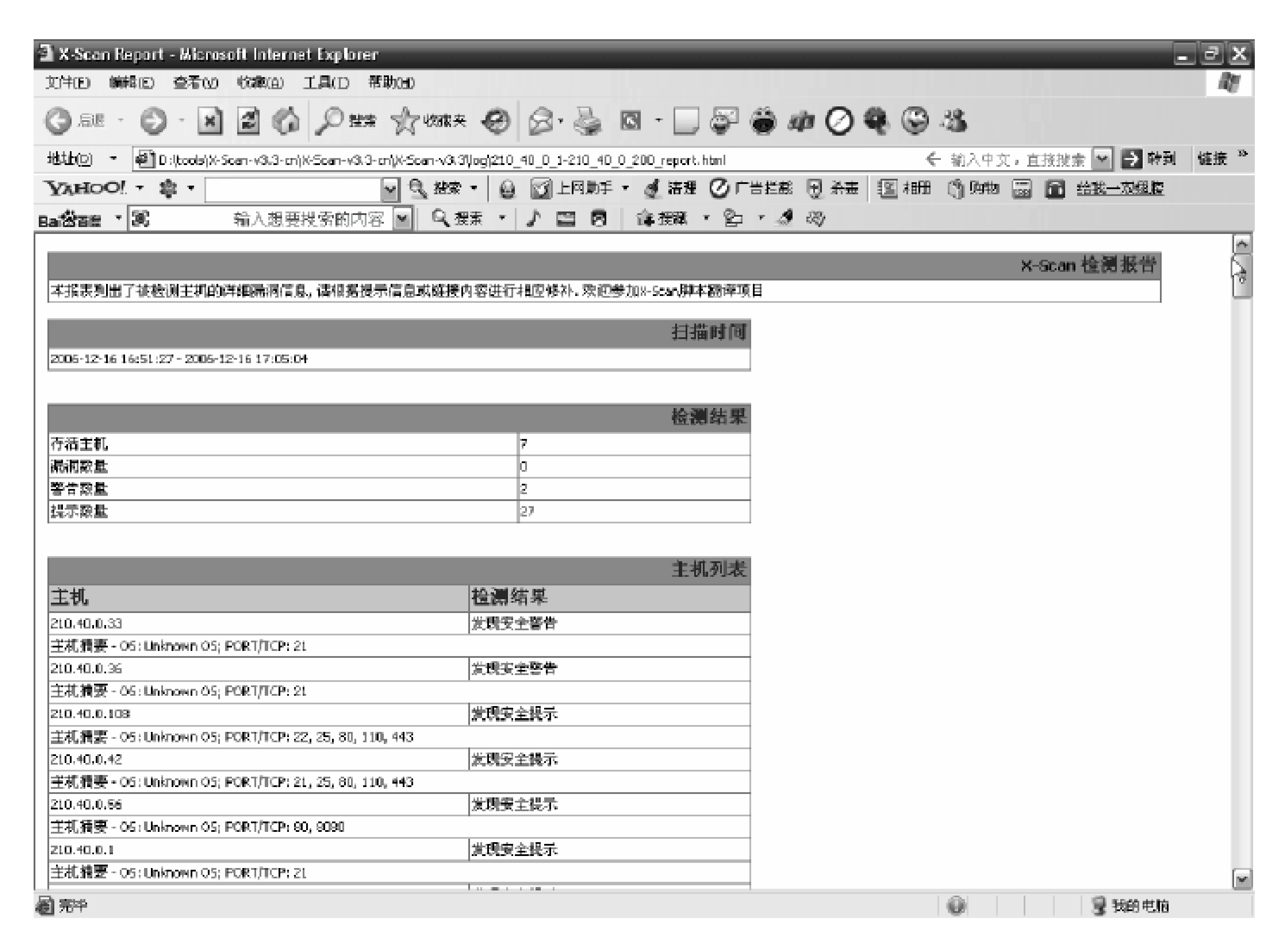


图 10-27 扫描结果报告

8. 工具

选择“工具”功能,进入工具操作界面,如图 10-28 所示。



图 10-28 工具操作界面

- “物理地址查询”选项卡。用以查询目标主机的 IP 地址、域名及物理网卡地址。
- ARP query 选项卡。用以查询目标主机 IP 地址与 MAC 地址的绑定情况。若不指定目标主机，则针对本机所在网段进行查询。
- Whois 选项卡。用以进行 Whois 查询。
- Trace route 选项卡。用以查询目标主机的路由情况，参见 10.2.1 小节的 Tracert 命令。
- ping 选项卡。用以进行 ping 查询，参见 10.2.1 小节的 ping 命令。

9. 命令行运行方式参数说明

1）命令格式

```
xscan -host <起始 IP> [-< 终止 IP>] <检测项目> [其他选项]
xscan -file <主机列表文件名><检测项目> [其他选项]
```

其中<检测项目> 含义如下：

-active：检测目标主机是否存活。

-os：　检测远程操作系统类型(通过 NETBIOS 和 SNMP 协议)。

-port：检测常用服务的端口状态。

-ftp：　检测 FTP 弱口令。

-pub：　检测 FTP 服务匿名用户写权限。

-pop3：检测 POP3-Server 弱口令。

-smtp：检测 SMTP-Server 漏洞。

-sql：　检测 SQL-Server 弱口令。

-smb：　检测 NT-Server 弱口令。

-iis：　检测 IIS 编码/解码漏洞。

-cgi：　检测 CGI 漏洞。

-nasl：　加载 Nessus 攻击脚本。

-all：　检测以上所有项目。

[其他选项] 含义如下：

-i <适配器编号>：设置网络适配器，<适配器编号>可通过－1 参数获取。

-l：显示所有网络适配器。

-v：显示详细扫描进度。

-p：跳过没有响应的主机。

-o：跳过没有检测到开放端口的主机。

-t <并发线程数量[,并发主机数量]>：指定最大并发线程数量和并发主机数量，默认数量为 100,10。

-log <文件名>：指定扫描报告文件名，以 TXT 或 HTML 作为后缀。

＊ cgi 及 iis 参数中“编码方案”含义如下：

用 HEAD 替换 GET。

用 POST 替换 GET。

用“GET / HTTP/1.0\r\nHeader:”替换 GET。

用“GET /[filename]? param=”替换 GET(可通过\dat\config.ini 文件的 CGI-ENCODE\encode4_index_file 项设置[filename])。

用“GET %00”替换 GET。

多个“/”或“\”、“/”与“\”互换。

用“＜Tab＞”替换“＜空格＞”。

注意,各变形方案若不冲突则可以同时使用,如-cgi 1,6,8 表示同时使用第 1、6、8 号方案对 HTTP 请求进行变形。

2) 示例

示例 1:xscan -host 210.50.0.10~210.50.0.254 -all -active -p

含义:检测网段 210.50.0.10~210.50.0.254 主机的所有漏洞,跳过无响应的主机。

示例 2:xscan -host 210.50.0.10~210.50.0.254 -port -smb -t 150 -o

含义:检测网段 210.50.0.10~210.50.0.254 主机的标准端口状态,NT 弱口令用户,最大并发线程数量为 150,跳过没有检测到开放端口的主机。

示例 3:xscan -file hostlist.txt -port -cgi -t 200,5 -v -o

含义:检测 hostlist.txt 文件中列出的所有主机的标准端口状态,CGI 漏洞,最大并发线程数量为 200,同一时刻最多检测 5 台主机,显示详细检测进度,跳过没有检测到开放端口的主机。

3) xscan 命令操作应用实例

对主机 10.1.23.11 进行扫描,目的是了解该主机开放了哪些端口。在 DOS 命令窗口下,执行下述命令:

```
xscan -host 10.1.23.11 -port
```

系统开始扫描,扫描结果如图 10-29 所示。

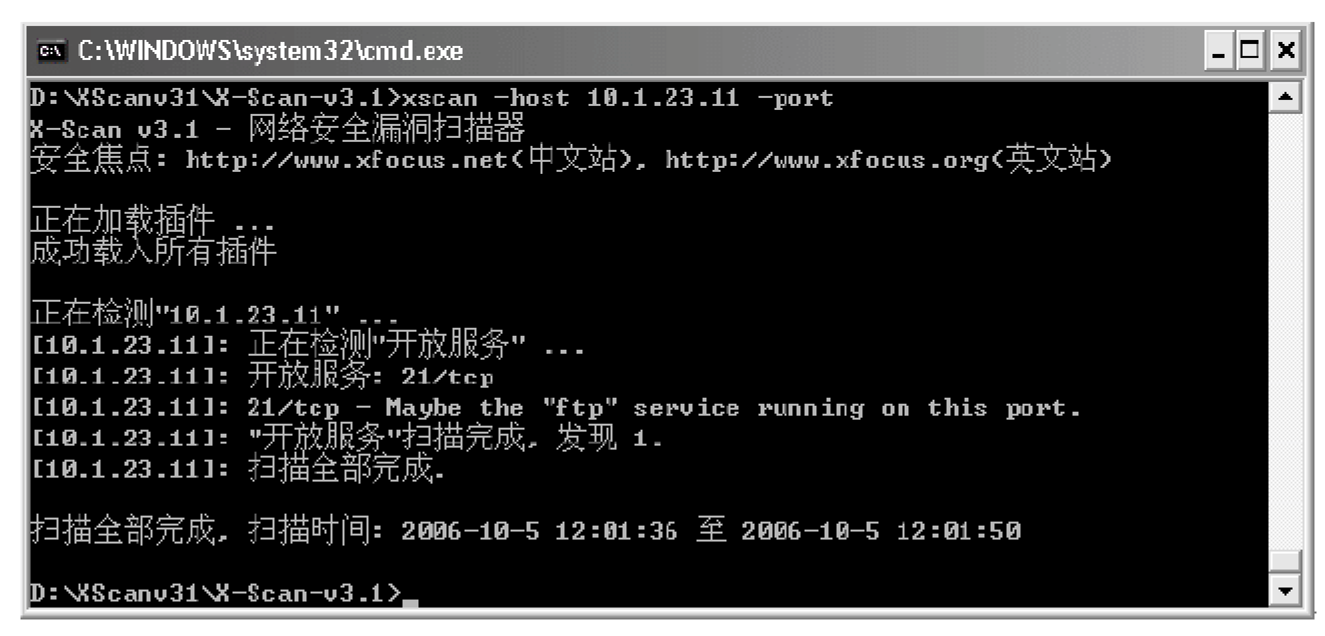


图 10-29 XSCAN 扫描结果

从图 10-29 的扫描可结果看出,主机 10.1.23.11 开放了一个端口 21,该端口用于 FTP 服务。

10.2.4 Namp

Nmap 是一款针对大型网络的端口扫描工具，它也适用于单机扫描。在不同情况下，用户可能需要隐藏扫描、越过防火墙扫描或者使用不同的协议进行扫描，比如 UDP、TCP、ICMP 等。它支持 Vanilla TCP connect 扫描、TCP SYN(半开式)扫描、TCP FIN、Xmas 或 NULL(隐藏)扫描、TCP ftp 代理(跳板)扫描、SYN/FIN IP 碎片扫描(穿越部分数据包过滤器)、TCP ACK 和窗口扫描、UDP 监听 ICMP 端口无法送达扫描、ICMP 扫描(狂 ping)、TCP Ping 扫描、直接 RPC 扫描(无端口映射)、TCP/IP 指纹识别远程操作系统以及相反身份认证扫描等。Namp 同时支持性能和可靠性统计，例如动态延时计算，数据包超时和转发，并行端口扫描，通过并行 ping 侦测下层主机等。由于本书篇幅所限，对 Namp 软件的操作过程不作详细介绍，有兴趣的读者可参阅有关资料。

10.3 应用实例

10.3.1 端口管理技术

1. 端口的分配

我们知道，一台拥有 IP 地址的主机可以提供许多服务，比如 Web 服务、FTP 服务和 SMTP 服务等，这些服务完全可以通过 1 个 IP 地址来实现。那么，主机怎样区分不同的网络服务呢？显然不能只靠 IP 地址，因为 IP 地址与网络服务的关系是一对多的关系。实际上是通过“IP 地址＋端口号”来区分不同的服务的。

需要注意的是，端口并不是一一对应的。比如用户的计算机作为客户机访问一台 WWW 服务器时，WWW 服务器使用的是 80 端口，用户的计算机则可使用 3457 端口，如图 10-30 所示。

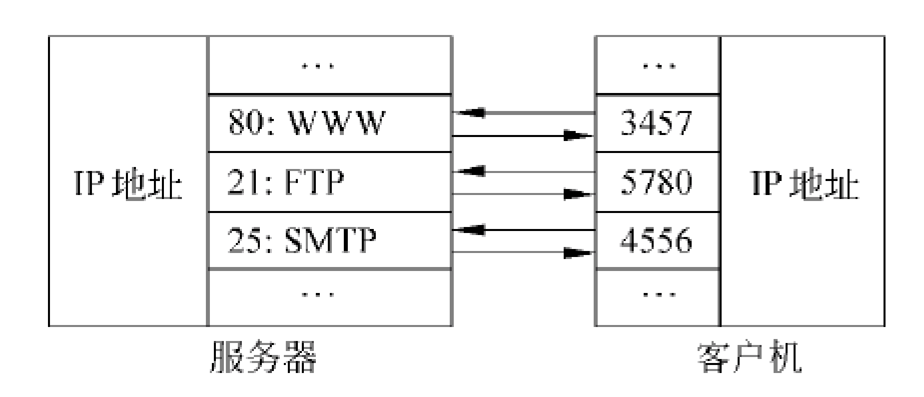


图 10-30 端口连接

按对应的协议类型分，端口有两种，TCP 端口和 UDP 端口。由于 TCP 和 UDP 两个协议是独立的，因此各自的端口号也相互独立，比如 TCP 有 235 端口，UDP 也可以有 235 端口。

2. 怎样查看端口

一台服务器有大量的端口在使用，怎么来查看端口呢？有两种方式：一种是利用系

统内置的命令，一种是利用第三方端口扫描软件。

（1）用系统内置命令 netstat-an 查看端口状态，Netstat 命令格式：

```
Netstat[-a][-e][-n][-o][-s][-an]
```

参数说明如下：

-a：表示显示所有活动的 TCP 连接以及计算机监听的 TCP 和 UDP 端口。

-e：表示显示以太网发送和接收的字节数、数据包数等。

-n：表示只以数字形式显示所有活动的 TCP 连接的地址和端口号。

-o：表示显示活动的 TCP 连接并包括每个连接的进程 ID(PID)。

-s：表示按协议显示各种连接的统计信息，包括端口号。

在 Windows 2000/XP 中，可以在命令提示符下使用 netstat -an 命令查看系统端口状态，可以列出系统正在开放的端口号及其状态，如图 10-31 所示。

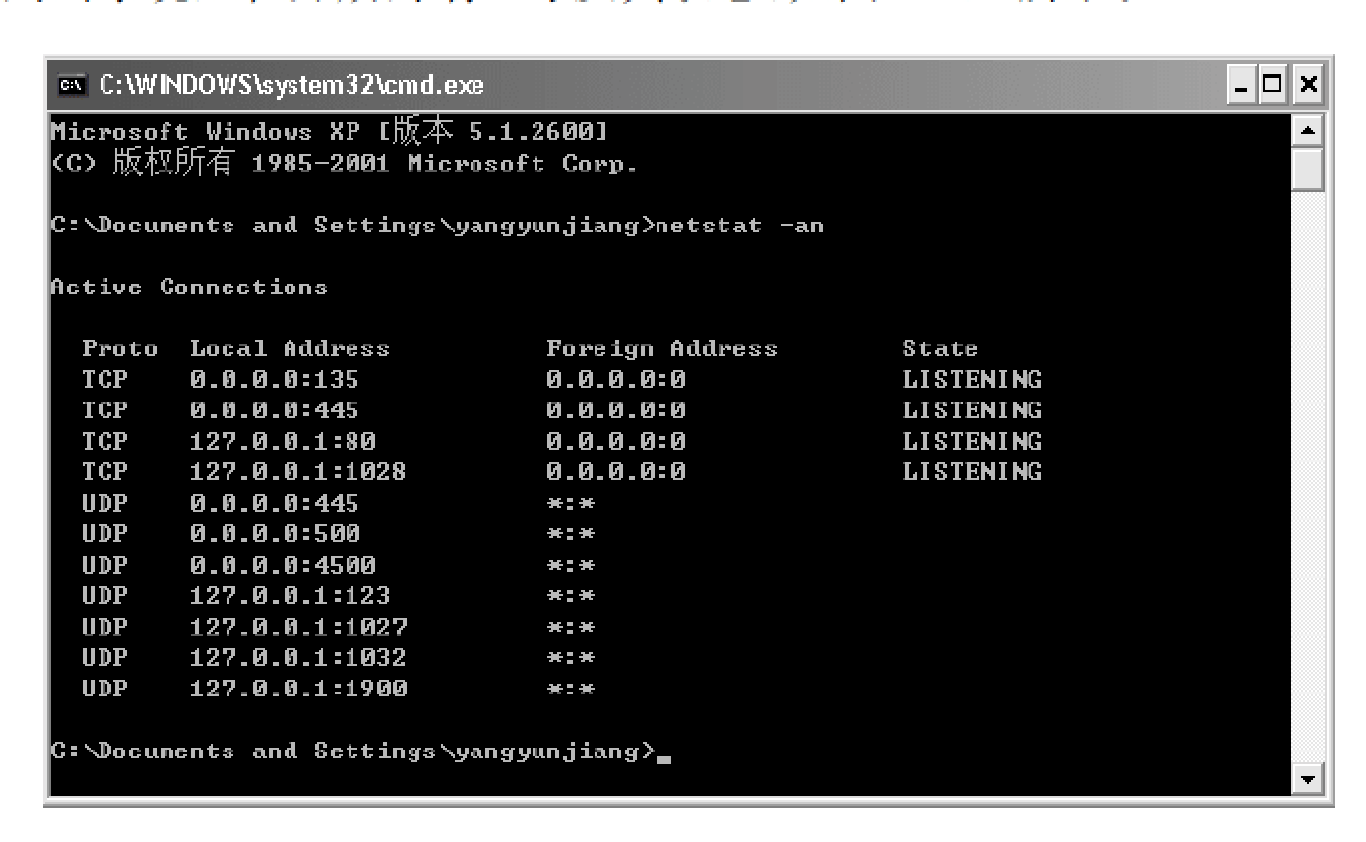


图 10-31 端口状态

（2）用第三方端口扫描软件。第三方端口扫描软件有很多种，界面虽然千差万别，但是功能却是相似的。这里以 Fport（可到 http://www.ccert.edu.cn/tools/index.php?type_t=7 或 http://www.ccidnet.com/soft/cce 下载）为例。Fport 在命令提示符下使用，运行结果与“netstat -an”相似，它不仅能够列出正在使用的端口号及类型，还可以列出端口正在被哪个应用程序使用，如图 10-32 所示。

3. 怎样管理端口

黑客程序是通过系统的端口漏洞来入侵系统的，因此对端口的管理是网管工作的一个非常重要的内容。管理端口可采用两种方法，一种方法是利用系统内置的管理工具，另一种方法是利用第三方软件来实现。

1）用“TCP/IP 筛选”管理端口

在 Windows 2000 Server/Windows XP 中，双击任务栏右下角的网络连接图标，再双击打开“本地连接状态”对话框，单击“属性”按钮，在选中“Internet 协议（TCP/IP）”后单

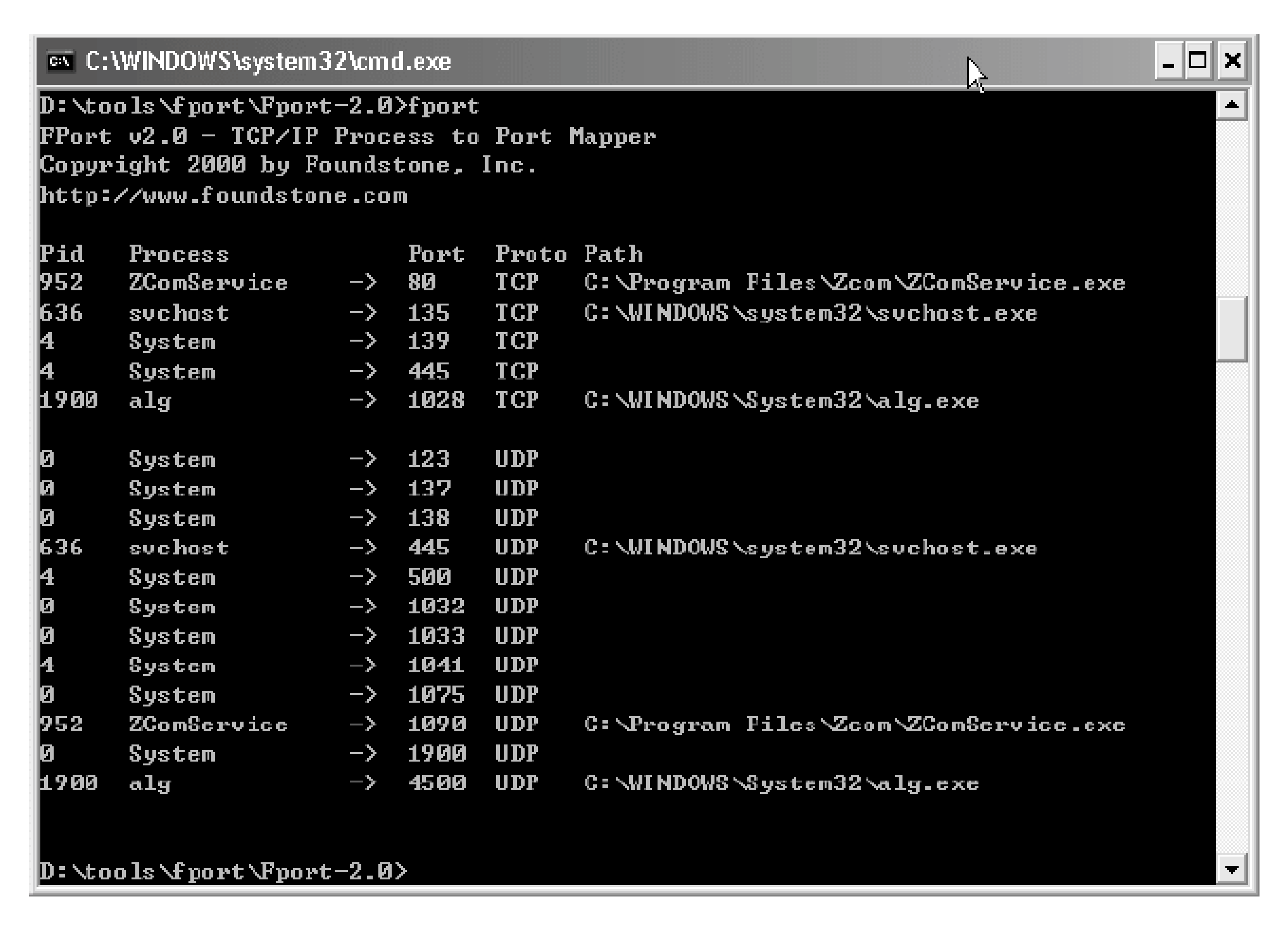


图 10-32 Fport 扫描结果

击“属性”按钮，在打开的“Internet 协议(TCP/IP)”对话框中单击“高级”按钮。在“高级TCP/IP 设置”中选择“选项”标签，选中“TCP/IP 筛选”，然后再单击“属性”按钮。在“TCP/IP 筛选”对话框里选择“启用 TCP/IP 筛选”的复选框，然后选择左边“TCP 端口”上的“只允许”选项。增加允许使用的端口，如 80、21、25 等，如图 10-33 所示，重新启动以后未经允许的端口就关闭了。



图 10-33 Windows 2000 Server/Windows XP 系统的端口管理

在图 10-33 中，可单击“添加”按钮添加端口，单击“删除”按钮删除端口。

2) 用第三方软件管理端口

管理端口最常用的第三方软件是防火墙软件。其实防火墙就是一整套制定好的 IP 地址及其端口的访问规则，用户可以通过改变这些规则来打开和关闭指定的端口。图 10-34 是瑞星个人防火墙的端口管理界面。

在图 10-34 中，“动作”栏打上“√”标记的为开放的端口，而打上“×”标记的为关闭的端口。可单击“增加规则”按钮来添加一条规则，单击“删除规则”来删除一条规则。

10.3.2 端口的关闭与开放

1. 端口的关闭和开放

在 Windows 的默认情况下，会有很多不安全的或无用的端口处于开启状态，比如



图 10-34　瑞星个人防火墙的端口管理

Telnet 服务的 23 端口、FTP 服务的 21 端口、SMTP 服务的 25 端口以及 RPC 服务的 135 端口等。为了保证系统的安全性，可以通过下面的方法来关闭/开启端口。

1）关闭端口

在 Windows 2000/XP 中关闭 Telnet 服务的端口，操作步骤为，首先打开“控制面板”，双击“管理工具”，再双击“服务”选项。接着在打开的服务窗口中找到并双击 Telnet 服务，如图 10-35 所示。



图 10-35　Windows 2000/XP 服务功能

在图 10-35 所示的屏幕中，单击“停止”按钮来停止该服务，然后在“启动类型”中选择

“已禁用”，最后单击“确定”按钮即可。这样，关闭了 SMTP 服务就相当于关闭了对应的端口，如图 10-36 所示。

2）开启端口

如果要开启该端口只需先在“启动类型”中选择“自动”选项，单击“确定”按钮，再打开该服务，在“服务状态”中单击“启动”按钮即可启用该端口，最后，单击“确定”按钮即可。

注意，在 Windows 98 中没有“服务”选项，可以使用防火墙的规则设置功能来关闭/开启端口。



图 10-36 Telnet 属性设置

2. 部分端口的关闭技术

1）113 端口木马的清除

这是一个基于 irc 聊天室控制的木马程序（仅适用于 Windows 系统）。

第 1 步，使用 netstat -an 命令确定自己的系统上是否开放了 113 端口。

第 2 步，使用 fport 命令查看出是哪个程序在监听 113 端口。

例如用 fport 命令看到如下结果：

```
Pid Process Port Proto Path
392 svchost ->  113 TCP C: \WINNT\system32\vhos.exe
```

就可以确定在监听 113 端口的木马程序是 vhos. exe，该程序所在的路径为 c：\winnt\system32。

第 3 步，确定了木马程序名（就是监听 113 端口的程序）后，在任务管理器中查找到该进程，并使用管理器结束该进程。

第 4 步，在“开始-运行”中输入 regedit，运行注册表管理程序，在注册表里查找刚才找到那个程序，并将相关的键值全部删掉。

第 5 步，到木马程序所在的目录下删除该木马程序（通常木马还会包括其他一些程序，如 rscan. exe、psexec. exe、ipcpass. dic、ipcscan. txt 等，根据木马程序不同，文件也有所不同，可以通过查看程序生成和修改的时间来确定与监听 113 端口的木马程序有关的其他程序）。

第 6 步，重新启动机器。

2）3389 端口的关闭

首先说明 3389 端口是 Windows 的远程管理终端所开的端口，它并不是一个木马程序，请先确定该服务是否是用户自己开放的。如果不是必需的，请关闭该服务。

（1）基于 Windows 2000 Server 的关闭方法。在 Windows 2000 Server 的“开始”|“程序”|“管理工具”|“服务”里找到 Terminal Services 服务项，选中属性选项将启动类型改成手动，并停止该服务。

(2) 基于 Windows XP 的关闭方法。在“我的计算机”上单击右键选择“属性”|“远程”，将里面的远程协助和远程桌面两个选项框里的“√”去掉。

3) 4899 端口的关闭

4899 端口是一个远程控制软件(remote administrator)服务端监听的端口，它不能算是一个木马程序，但是具有远程控制功能，通常杀毒软件是无法查出它来的，请先确定该服务是否是用户自己开放并且是必须开放的，如果不是请关闭它。

关闭 4899 端口。

选择“开始”|“运行”命令，在出现的对话框中输入 cmd(Windows 9x 为 command)，在 DOS 命令窗口下输入命令：cd c：\winnt\system32(系统安装目录)，输入 r_server. exe /stop 后按 Enter 键。然后在输入 r_server /uninstall /silence 到 c：\winnt\system32(系统目录)下删除 r_server. exe、admdll. dll 和 radbrv. dll 3 个文件。

4) 5800 和 5900 端口的关闭

第 1 步，首先使用 fport 命令确定出监听在 5800 和 5900 端口的程序所在位置(通常会是 c：\winnt\fonts\explorer. exe)。

第 2 步，在任务管理器中关掉相关的进程(注意有一个是系统本身正常的，请注意：如果错关可以重新运行 c：\winnt\explorer. exe)。

第 3 步，删除 c：\winnt\fonts\中的 explorer. exe 程序。

第 4 步，删除注册表 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 中的 Explorer 项。

第 5 步，重新启动机器。

5) 6129 端口的关闭

6129 端口是一个远程控制软件(dameware nt utilities)服务端监听的端口，它不是一个木马程序，但是具有远程控制功能，一般的杀毒软件是无法查出的。请先确定该服务是否是用户自己安装并且是必需的，如果不是请关闭。

关闭 6129 端口。

选择“开始”|“设置”|“控制面板”|“管理工具”|“服务”。找到 DameWare Mini Remote Control 项单击右键选择属性选项，将启动类型改成禁用后停止该服务。到 c：\winnt\system32(系统目录)下将 DWRCS. EXE 程序删除，到注册表内将 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\DWMRCS 表项删除。

6) 1029 端口和 20168 端的关闭

这两个端口是 lovgate 蠕虫所开放的后门端口。

蠕虫相关信息请参见 Lovgate 蠕虫。http：//it. rising. com. cn/newSite/Channels/anti_virus/Antivirus_Base/TopicExplorerPagePackage/lovgate. htm。

用户可以下载专杀工具 http：//it. rising. com. cn/service/technology/RS_LovGate_download. htm。

使用方法：下载后直接运行，在该程序运行结束后重启计算机后再运行一遍该程序。

7) 45576 端口的关闭

这是一个代理软件的控制端口，请先确定该代理软件并非用户自己安装的(代理软

件会给用户的机器带来额外的流量)。

关闭以下代理软件:

- 请先使用 fport 查看出该代理软件所在的位置。
- 在服务中关闭该服务(通常为 SkSocks),将该服务关掉。
- 到该程序所在目录下将该程序删除。

习 题 10

1. 在网络系统中,端口指的是什么?
2. 网络端口如何进行分类?
3. 端口扫描的基本原理是什么?
4. 端口扫描器的主要用途是什么?
5. 端口扫描器的主要能力是什么?

第 11 章 chapter 11

嗅探技术

11.1 网络协议分析及嗅探原理

11.1.1 嗅探技术与嗅探器

嗅探器(sniffer)可以理解为一个安装在计算机上的窃听设备,它可以用来窃听计算机在网络上所产生的众多的信息。一部电话的窃听装置,可以用来窃听双方通话的内容,而计算机网络嗅探器则可以窃听计算机程序在网络上发送和接收到的数据。

嗅探器是利用计算机的网络接口截获目的地及其他计算机数据报文的一种技术。它工作在网络的最底层,把网络传输的全部数据记录下来。嗅探器可以帮助网络管理员查找网络漏洞和检测网络性能,嗅探器可以分析网络的流量,以便找出所关心的网络中潜在的问题。不同传输介质的网络可监听性是不同的。一般来说,以太网被监听的可能性比较高,因为以太网是一个广播型的网络;FDDI Token 被监听的可能性也比较高,尽管它并不是一个广播型网络,但带有令牌的那些数据包在传输过程中,平均要经过网络上一半的计算机;微波和无线网被监听的可能性同样比较高,因为无线电本身是一个广播型的传输介质,弥散在空中的无线电信号可以被很轻易地截获。一般情况下,大多数的嗅探器至少能够分析下面的协议:

- 标准以太网协议。
- TCP/IP。
- IPX。
- DECNET。
- FDDI Token。
- 微波和无线网协议。

实际应用中的嗅探器分软、硬件两种。软件嗅探器便宜、易于使用,缺点是往往无法抓取网络上所有的传输数据(比如碎片),也就无法全面了解网络的故障和运行情况;硬件嗅探器通常称为协议分析仪,它的优点恰恰是软件嗅探器的缺点,但是价格昂贵。目前使用的嗅探器仍是以软件为主。

嗅探器捕获真实的网络报文。嗅探器通过将其置身于网络接口来达到这个目的。例如,将以太网卡设置成混杂模式。数据在网络上是以帧(frame)为单位传输的,帧是通

过特定的网络驱动程序进行传送的，然后通过网卡发送到网线上。通过网线到达它们的目的机器，在目的机器的一端执行相反的过程。接收端机器的以太网卡捕获到这些帧，并告诉操作系统帧已到达，然后对其进行存储。就是在这个传输和接收的过程中，每一个在 LAN 上的工作站都有其硬件地址。这些地址唯一地表示网络上的机器。当用户发送一个报文时，这些报文就会发送到 LAN 上所有可用的机器中。在一般情况下，网络上所有的机器都可以“侦听”到通过的流量，但对不属于自己的报文则不予响应。如果某工作站的网络接口处于混杂模式，那么它就可以捕获网络上所有的报文和帧，如果一个工作站被配置成这样的方式，它就是一个嗅探器。这也是嗅探器会造成安全方面问题的原因。通常使用嗅探器的入侵者，都必须拥有基点来放置嗅探器。对于外部入侵者来说，能通过入侵外网服务器、往内部工作站发送木马等方式获得所需信息，然后用基点来放置其嗅探器，而内部破坏者就能够直接获得嗅探器的放置点，比如使用附加的物理设备作为嗅探器。嗅探器可能造成的危害如下：

- 嗅探器能够捕获口令。
- 能够捕获专用的或者机密的信息。
- 可以用来危害网络邻居的安全，或者用来获取更高级别的访问权限。
- 分析网络结构，进行网络渗透。

11.1.2 通信协议分析

1. 与嗅探技术有关的网络通信设备

- 中继器。中继器的主要功能是终结一个网段的信号并在另一个网段再生该信号，起到信号放大和转发的作用，中继器工作在物理层上。
- 网桥。网桥使用 MAC 物理地址实现中继功能，可以用来分隔网段或连接部分异种网络，网桥工作在数据链路层。
- 路由器。路由器工作在网络层，主要负责数据包的路由寻径，也能处理物理层和数据链路层上的工作。
- 网关。主要工作在网络第 4 层以上，主要实现收敛功能及协议转换，不过很多时候网关都被用来描述任何网络互连设备。

2. TCP/IP 与以太网

以太网和 TCP/IP 可以说是相辅相成的，可以说两者的关系几乎是密不可分的，以太网在 1、2 层提供物理上的连线，而 TCP/IP 工作在上层，使用 32 位的 IP 地址，以太网则使用 48 位的 MAC 地址，两者间使用 ARP 和 RARP 协议进行相互转换。

载波监听/冲突检测(CSMA/CD)技术被普遍使用在以太网中，所谓载波监听是指在以太网中的每个站点都具有同等的权利，在传输自己的数据时，首先监听信道是否空闲，如果空闲，就传输自己的数据，如果信道被占用，就等待信道空闲。而冲突检测则是为了防止发生两个站点同时在网络发送数据而产生的冲突。以太网采用广播机制，所有与网络连接的工作站都可以看到网络上传递的数据。

3. TCP/IP 通信

在 TCP/IP 通信中，网络接口层直接与硬件地址相连接，网间网层与 IP 地址相连接，传输层与 TCP 接口相连接，应用层则是面向用户的应用程序接口，如 FTP、Telnet 等接口。一个典型的在以太网中客户与服务器使用 TCP/IP 协议的通信如图 11-1 所示。

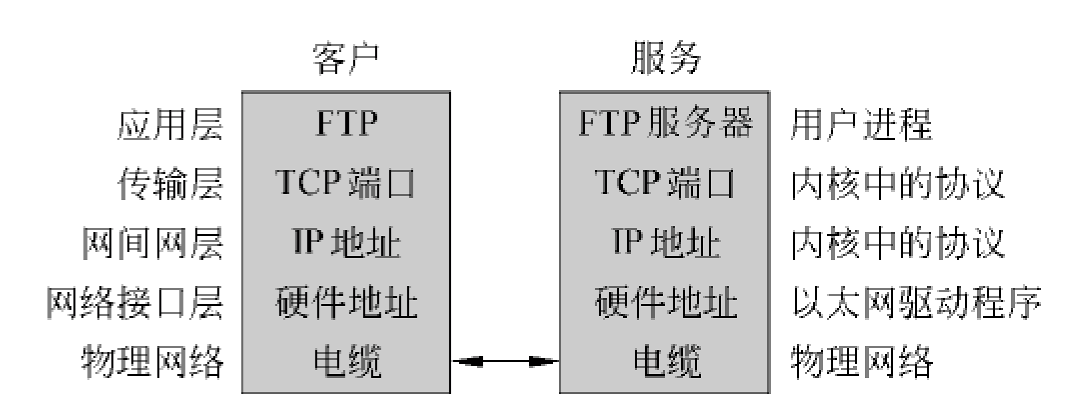


图 11-1 TCP/IP 通信拓扑图

11.1.3 嗅探原理

我们知道，计算机所传送的数据是大量的二进制数据。因此，一个网络窃听程序也必须使用特定的网络协议来分析嗅探到的数据，嗅探器也就必须能够识别出哪个协议对应于这个数据片断，只有这样才能够进行正确的解码。

网络嗅探器比起电话窃听器来说，有它独特的优势，很多的计算机网络采用的是“共享媒体”。几乎可以在任何连接着的网络上直接窃听到同一掩码范围内的计算机网络数据，这种窃听方式称为“基于混杂模式的嗅探”(promiscuous mode)。

我们知道，在以太网中，所有的通信都是广播方式，也就是说通常在同一个网段的所有网络接口都可以接收在物理媒体上传输的所有数据，而每一个网络接口都有一个唯一的硬件地址，这个硬件地址也就是网卡的 MAC 地址，MAC 使用的是 48 比特的地址，这个地址用来表示网络中的每一个设备，每块网卡上的 MAC 地址都是不同的。在硬件地址和 IP 地址间使用 ARP 和 RARP 协议进行相互转换。

在正常的情况下，一个网络接口应该只通过响应下述的两种数据帧来完成：

- 与自己硬件地址相匹配的数据帧。
- 发向所有机器的广播数据帧。

网卡接收到传输来的数据，网卡内的单片程序接收数据帧的目的 MAC 地址，根据计算机上的网卡驱动程序设置的接收模式判断该不该接收，认为该接收就在接收后产生中断信号通知 CPU，认为不该接收就丢掉不管，所以不该接收的数据在网卡处就截断了，计算机根本就不知道。CPU 得到中断信号产生中断，操作系统就根据网卡的驱动程序设置的网卡中断程序地址调用驱动程序接收数据，驱动程序接收数据后放入信号堆栈让操作系统处理。而对于网卡来说一般有 4 种接收模式。

- 广播方式。该模式下的网卡能够接收网络中的所有广播信息。
- 组播方式。设置在该模式下的网卡能够接收组播数据。
- 直接方式。在这种模式下，只有目的网卡才能接收该数据。

- 混杂模式。在这种模式下的网卡能够接收一切通过它的数据，而不管该数据是否是传给它的。

与 HUB 只是简单地把所接收到的信号通过所有端口重复发送出去不同，Switch 却可以检查每一个收到的数据包，并对数据包进行相应的处理。在 Switch 内保存着每一个网段上所有结点的物理地址，只允许必要的网络流量通过 Switch。举例来说，当 Switch 接收到一个数据包之后，根据自身保存的网络地址表检查数据包内包含的发送方和接收方地址。如果接收方位于发送方网段内，该数据包就会被 Switch 丢弃，不能通过交换机传送到其他的网段；如果接收方和发送方位于两个不同的网段，该数据包就会被 Switch 转发到目标网段。这样，通过交换机的过滤和转发，可以有效避免网络广播风暴，减少误包和错包的出现。

通过前面的学习，网卡接收信息技术可总结如下：

- 在以太网中是基于广播方式传送数据的，也就是说，所有的物理信号都要经过连接在以太网段上的机器。
- 网卡可以置于混杂模式(promiscuous)，在这种模式下工作的网卡能够接收到一切通过它的数据，而不管实际上数据的目的地址是不是自己的。这实际上就是 Sniff 工作的基本原理，让网卡接收一切能接收的数据。

来看一个简单的例子，如图 11-2 所示，机器 A、B、C 与集线器 HUB 相连接，集线器 HUB 通过路由器 Router 访问外部网络。

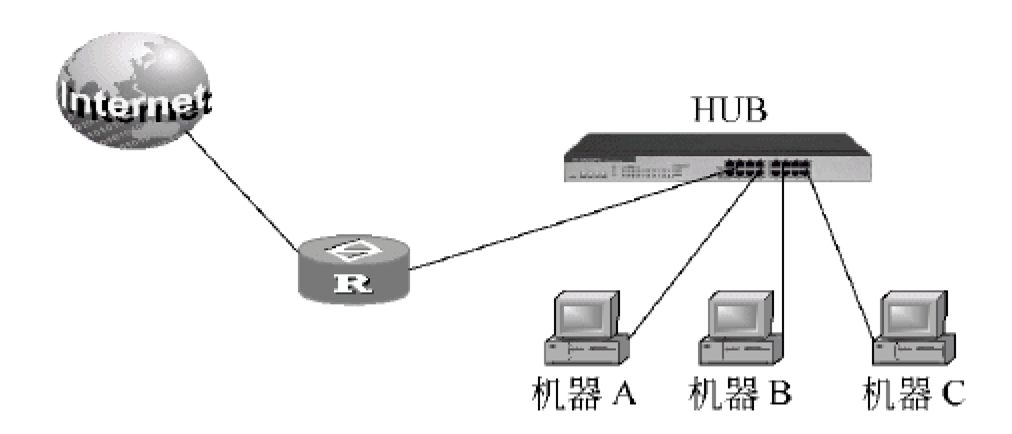


图 11-2　一个简单的以太拓扑图

值得注意的一点是机器 A、B、C 使用一个普通的 HUB 连接的，不是用 Switch，也不是用 Router，使用 Switch 和 Router 的情况要比这复杂得多。

假设机器 A 上的管理员为了维护机器 C，使用了一个 FTP 命令向机器 C 进行登录，那么在这个用 HUB 连接的网络里数据走向过程是这样的。首先机器 A 上的管理员输入的登录机器 C 的 FTP 命令经过应用层 FTP 协议、传输层 TCP 协议、网络层 IP 协议和数据链路层上的以太网驱动程序一层一层的包裹，最后送到了物理层所连接的网线上，如图 11-3 所示。接下来数据帧送到了 HUB 上，再由 HUB 向每一个接点广播由机器 A 发出的数据帧，机器 B 接收到由 HUB 广播发出的数据帧，并检查在数据帧中的地址是否和自己的地址相匹配，发现不是发向自己的数据后就把这数据帧丢弃，不予理睬。而机器 C 也接收到了数据帧，并在比较之后发现是自己的数据帧，接下来就对这数据帧进行接收和分析处理。

在这个简单的例子中，机器 B 上的管理员如果很好奇，想知道究竟登录机器 C 上 FTP

口令是什么，要做的事情是很简单的，仅仅需要把自己机器上的网卡置于混杂模式，即可接收数据，接着对接收到的数据帧进行分析，从而可得到包含在数据帧中所想知道的信息。

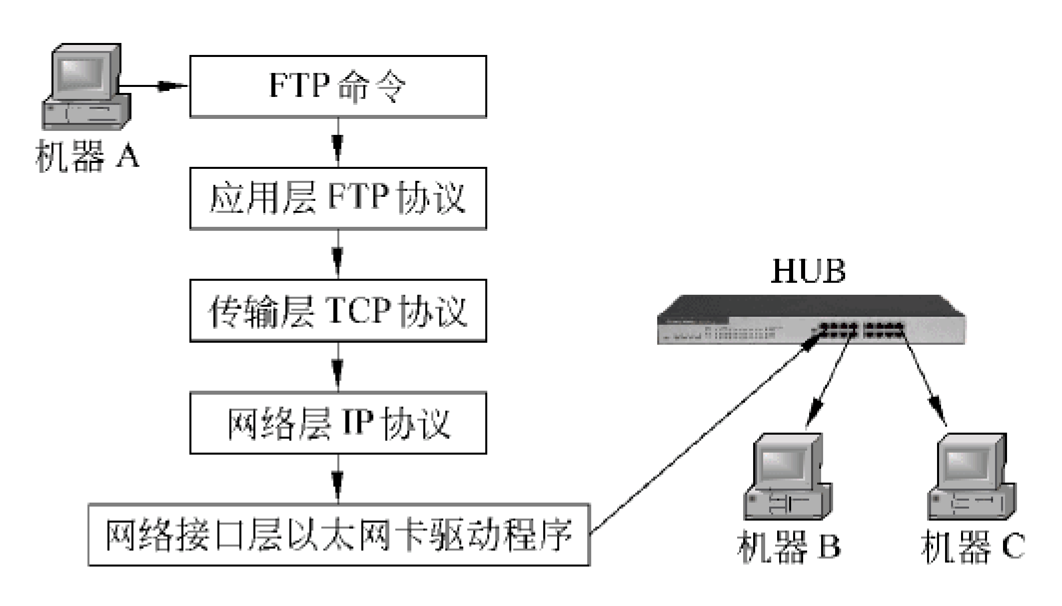


图 11-3　FTP 命令执行过程

11.1.4　简单的嗅探技术

本小节介绍几种常用的嗅探技术。

1. ARP Spoof(ARP 欺骗)

ARP Spoof 攻击的根本原理是因为计算机中维护着一个 ARP 高速缓存，并且这个 ARP 高速缓存是随着计算机不断的发出 ARP 请求和收到 ARP 响应而不断地更新的，ARP 高速缓存的目的是把机器的 IP 地址和 MAC 地址相互映射(绑定)。可以使用 ARP 命令来查看自己的 ARP 高速缓存。现在设想一下，一个 Switch 工作在数据链路层，根据 MAC 地址来转发它所接收的数据包，而计算机维护的 ARP 高速缓存却是动态的。在这种情况下，会发生什么样的事情呢？

为了便于分析，在此为 3 台计算机统一分配 IP 地址。

假设机器 A 的 IP 地址为 10.0.0.1，MAC 地址为 20-53-52-43-00-01，机器 B 的 IP 地址为 10.0.0.2，MAC 地址为 20-53-52-43-00-02，机器 C 的 IP 地址为 10.0.0.3，MAC 地址为 20-53-52-43-00-03。

现在机器 B 上的管理员想窃取机器 A 向机器 C 发送的信息，他向机器 A 发出一个 ARP Reply (ARP 应答)，其中目的 IP 地址为 10.0.0.1，目的 MAC 地址为 20-53-52-43-00-01，而源 IP 地址为 10.0.0.3，源 MAC 地址为 20-53-52-43-00-02，机器 A 收到 ARP 命令信息后就会及时更新它的 ARP 高速缓存的内容，并相信了 IP 地址为 10.0.0.3 的机器的 MAC 地址是 20-53-52-43-00-02。当机器 A 上的管理员发出一条 FTP 命令 ftp 10.0.0.3(其本意是用 FTP 命令登录机器 C)时，数据包即被送到了 Switch，Switch 查看数据包中的目的地址，发现 MAC 为 20-53-52-43-00-02，于是，就把数据包发到了机器 B 上。这就是典型的 ARP 欺骗技术。

2. MAC Flooding(MAC 地址溢出)

在上面曾经提到过，Switch 之所以能够由数据包中目的 MAC 地址判断出它应该把

数据包发送到哪一个端口上，是根据自身维护的一张 ARP 地址表。这张地址表可能是动态的也可能是静态的，这要看 Switch 的厂商和 Switch 的型号来定，对于某些 Switch 来说，它维护的是一张动态的地址表，并且地址表的大小是有上限的，比如 3com Superstack Switch 3300 就是这样一种 Switch，可以通过发送大量错误的地址信息而使 Switch 维护的地址表“溢出”，从而使它变成广播模式来达到所要 Sniff 机器 A 与机器 C 之间的通信的目的。

3. Fake the MAC address（伪造 MAC 地址）

伪造 MAC 地址也是一种常用的办法，不过这要基于用户网络内的 Switch 是动态更新其地址表，这实际上和上面说到的 ARP Spoof 有些类似，只不过现在是想要 Switch 相信用户，而不是要机器 A 相信用户。因为 Switch 是动态更新其地址表的。其关键技术是需要向 Switch 发送伪造过的数据包，其中源 MAC 地址对应的是机器 C 的 MAC 地址，现在 Switch 就把机器 C 和用户的端口对应起来了。

4. ICMP Router Advertisements（ICMP 路由通告）

这主要是由 ICMP 路由器发现协议（IRDP）的缺陷引起的，在 Windows 95/98/2000 及 Sun OS、Solaris 2.6 等系统中，都使用了 IRDP 协议，Sun OS 系统只在某些特定的情况下使用该协议，而 Windows 95/98 和 Windows 2000 都是默认的使用 IRDP 协议。IRDP 协议的主要内容就是告诉人们谁是路由器，如果一个黑客利用 IRDP 宣称自己是路由器的情况是很糟糕的，因为所有相信黑客请求的机器都会把所有的数据都发送给黑客所控制的机器。

5. ICMP Redirect（ICMP 重定向）

所谓 ICMP 重定向，就是指告诉机器向另一个不同的路由发送它的数据包，ICMP 重定向通常使用在这样的场合下，假设 A 与 B 两台机器分别位于同一个物理网段内的两个逻辑子网内，而 A 和 B 都不知道这一点，只有路由器知道，当 A 发送给 B 的数据到达路由器的时候，路由器会向 A 送一个 ICMP 重定向包，将 B 的真实地址告诉 A，这样，A 就可以和 B 直接通信了。而一个黑客完全可以利用这一点来进行攻击，使得 A 发送给 B 的数据直接发送给黑客。

11.2 常用嗅探器

现在网络上经常使用的 Sniff 有基于 Windows 环境下的 Sniff 和基于 UNIX 环境下的 Sniff。

基于 Windows 环境下的 Sniff 有 netxray 以及 Sniffer pro，基于 UNIX 环境下 Sniff 有 Sniffit、Snoop、TCPdump 和 Dsniff 等。

11.2.1 Sniffit

Sniffit 可以运行在 Solaris、SGI 和 Linux 等平台上，由 Lawrence Berkeley Laboratory 实验室开发的一个免费的网络监听软件。而 Sniffit PRO 版支持 Windows NT，也支持 Windows 2000。

使用方法如下：

-a：以 ASCII 形式将监听的结果输出。

-A：在进行记录时，所有不可打印的字符都可代替。

-b：等同于同时使用参数-t & -s。

-d：将监听所得内容以十六进制方式显示在当前终端。

-p：记录连接到的包，0 为所有端口。默认为 0。

-P protocol：选择要检查的协议，默认为 TCP。可能的选择有 IP、TCP、ICMP、UDP 和它们的组合。

-s：指定 Sniffer 检查发送的数据包。

-t：指定 Sniffer 检查发送到的数据包。

-i：进入交互模式。

-l：设定数据包大小，default（默认值）是 300 字节。

例如：

想要记录从主机 210.50.30.100 上的用户口令：

```
sniffit: ~ /# sniffit -p 23 -t 210.50.30.100
```

想要记录到主机 210.50.30.100 的 ftp 服务：

```
sniffit: ~ /# sniffit -p 21 -l 0 -t 210.50.30.100
```

记录所有发出和发往主机 210.50.30.100 的电子邮件信息：

```
sniffit: ~ /# sniffit -p 25 -l 0 -b -t 210.50.30.100
```

或者

```
sniffit: ~ /# sniffit -p 25 -l 0 ;-b ;-s ;210.50.30.100
```

想要使用有菜单的界面：

```
sniffit: ~ /# sniffit -i
```

网络出现一些错误，想要查看控制消息：

```
sniffit: ~ /# sniffit -p icmp -b -s 210.50.30.100
```

将口令记录在以 nnn 开始的文件中，可以用 cat nnn* 来查看：

```
sniffit: ~ /# sniffit -p 23 -A . -t 210.50.30.100
```

或者

```
sniffit: ~ /# sniffit -p 23 -A ^ -t dummy.net
```

下面是运行 sniffit 的一个例子。

```
# sniffit -a -A . -p 23 -t 11.22.33.14
```

入口参数的设置非常简单,为-a 接收所有信息;-A 将不可打印字符用“.”代替;-p 监听端口 23;-t 目标地址在 11.22.33 子网范围(可以只监听一台主机或者是源主机),使用-s 参数可以指定监听的源主机。网络监听程序的入口参数其实非常简单,只要具有初步的网络知识便可以正确地使用它们。以下是监听到的部分结果。

```
Packet D rom 1P.port-to P.port: 11. 22.33.41.1028-11.22.33.14.23
E..35.0. ....!.(.......K.2.P."/.: ....vt100..
```

出现 vtl00 的字样,是使用 Telnet 服务时,源主机与目标主机进行终端类型协商,在这一阶段源主机告诉目标主机自己使用的终端类型,这是一次远程终端服务的开始。在这之后,很可能就会传输用户的登录名和口令字。这里很清楚,使用端口 1028 的是客户端,而使用端口 23 的是服务器端。

11.2.2 Snoop

Snoop 默认情况安装在 Solaris 下,是一个用于显示网络交通的程序。

使用方法如下:

```
[ -a ]: Listen to packets on audio
[ -d device ]: settable to le,ie,bf,tr
[ -s snaplen ]: Truncate packets
[ -c count ]: Quit after count packets
[ -P ]: Turn OFF promiscuous mode
[ -D ]: Report dropped packets
[ -S ]: Report packet size
[ -i file ]: Read previously captured packets
[ -o file ]: Capture packets in file
[ -n file ]: Load addr-to-name table from file
[ -N ]: Create addr-to-name table
[ -t r|a|d ]: Time: Relative, Absolute or Delta
[ -v ]: Verbose packet display
[ -V ]: Show all summary lines
[ -p first[,last] ]: Select packet(s) to display
[ -x offset[,length] ]: Hex dump from offset for length
[ -C ]: Print packet filter code
```

11.2.3 TCPdump

1. TCPdump 命令格式

TCPdump 采用命令行方式,它的命令格式为:

TCPdump [-adeflnNOpqStvx][-c 数量][-F 文件名][-i 网络接口][-r 文件名][-s snaplen][-T 类型][-w 文件名][表达式]

2. TCPdump 的选项

-a：将网络地址和广播地址转变成名字。
-d：将匹配信息包的代码以人们能够理解的汇编格式给出。
-dd：将匹配信息包的代码以 C 语言程序段的格式给出。
-ddd：将匹配信息包的代码以十进制的形式给出。
-e：在输出行打印出数据链路层的头部信息。
-f：将外部的 Internet 地址以数字的形式打印出来。
-l：使标准输出变为缓冲行形式。
-n：不把网络地址转换成名字。
-t：在输出的每一行不打印时间戳。
-v：输出一个稍微详细的信息，例如在 IP 包中可以包括 TTL 和服务类型的信息。
-vv：输出详细的报文信息。
-c：在收到指定的包的数目后，TCPdump 就会停止。
-F：从指定的文件中读取表达式，忽略其他的表达式。
-i：指定监听的网络接口。
-r：从指定的文件中读取包(这些包一般通过-w 选项产生)。
-w：直接将包写入文件中，并不分析和打印出来。
-T：将监听到的包直接解释为指定的类型的报文，常见的类型有 rpc 和 snmp。

3. TCPdump 的表达式

表达式是一个条件表达式，TCPdump 利用它作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会被截获。

在表达式中一般有如下几种类型的关键字，第一种是关于类型的关键字，主要包括 host、net 以及 port，例如 host 210.27.48.2，指明 210.27.48.2 是一台主机，net 202.0.0.0 指明 202.0.0.0 是一个网络地址，port 23 指明端口号是 23。如果没有指定类型，默认的类型是 host。

第二种是确定传输方向的关键字，主要包括 src、dst、dst or src 以及 dst and src，这些关键字指明了传输的方向。举例说明，src 210.27.48.2，指明 IP 包中源地址是 210.27.48.2，dst net 202.0.0.0 指明目的网络地址是 202.0.0.0。如果没有指明方向关键字，则默认是 src or dst 关键字。

第三种是协议的关键字，主要包括 fddi、ip、arp、rarp、tcp 和 udp 等类型。fddi 指明是在 FDDI(分布式光纤数据接口网络)上的特定的网络协议，实际上它是 Ether 的别名，FDDI 和 Ether 具有类似的源地址和目的地址，所以可以将 FDDI 协议包当作 Ether 的包进行处理和分析，其他的几个关键字就是指明了监听的包的协议内容。如果没有指定任

何协议，则 TCPdump 将会监听所有协议的信息包。

除了这 3 种类型的关键字之外，其他重要的关键字如下：

gateway、broadcast、less、greater，还有三种逻辑运算，“非”运算是 not 和“!”；“与”运算是 and 和“&&”；“或”运算是 or 和“||”。

例如：

```
#TCPdump host 210.40.10.133
```

将监听 IP 地址为 210.40.0.133 的机器的通话。

```
#TCPdump host 210.40.10.133 and 210.40.10.135
```

将监听 IP 地址为 210.40.0.133 及 IP 地址为 210.40.10.135 的机器的通话。

```
#TCPdump tcp port 23 host 210.40.10.133
```

将监听 IP 地址为 210.40.10.133 的机器的 23 端口的通话。

11.2.4 Dsniff

Dsniff 不仅仅是一个 sniff，在它的整个套件包中，包含了很多其他有用的工具，如 arpspoof、dnsspoof、macof 和 tcpkill 等，比 Sniff 的手段更加的多样和复杂化。Dsniff 是由 DugSong 开发的。目前 Dsniff 支持 OpenBSD (i386)、Redhat Linux(i386)和 Solaris (sparc)，并且在 FreeBSD、Debian Linux、Slackware Linux、AIX 和 HP-UX 上也能运转得很好。但是 Dsniff 需要几个其他的第三方软件进行支持，它们分别是 Berkeley DB、OpenSSL、libpcap、libnet 和 libnids。

11.3 网络嗅探防范技术

11.3.1 如何在网络上发现 Sniffer

检测嗅探器可以采用检测混杂模式网卡的工具。由于嗅探器需要将网络中入侵的网卡设置为混杂模式才能工作，能够检测混杂模式网卡的 AntiSniff 是一个工具。证明网络被嗅探有以下 3 种方法：

1. 网络通信丢包率非常高

通过一些网管软件，可以看到信息包传送情况，最简单是 ping 命令。它会告诉用户掉了百分之多少的包。如果用户的网络结构正常，而又有 20%～30%数据包丢失以致数据包无法顺畅的流到目的地。就有可能有人在监听，这是由于嗅探器拦截数据包导致的。

2. 网络带宽出现反常

通过某些带宽控制器，可以实时看到目前网络带宽的分布情况，如果某台机器长时

间的占用了较大的带宽，这台机器就有可能在监听。应该也可以察觉出网络通信速度的变化。

对于 SunOS 和其他 BSD UNIX 系统可以使用 lsof 来检测嗅探器的存在。lsof 最初的设计目的并非为了防止嗅探器入侵，但因为在嗅探器入侵的系统中，嗅探器会打开其输出文件，并不断传送信息给该文件，这样该文件的内容就会越来越大。如果利用 lsof 发现有文件的内容不断的增大，就怀疑系统被嗅探。因为大多数嗅探器都会把截获的"TCP/IP"数据写入自己的输出文件中。这里可以用 ifconfig le0 检查端口，然后用：

```
# /usr/sbin/lsof> test
# vi test 或 grep[打开的端口号]
```

检测文件大小的变化。

注意，如果用户确信有人接了嗅探器到自己的网络上，可以去找一些进行验证的工具，这种工具称为时域反射计量器（Time Domain Reflectometer，TDR）。TDR 对电磁波的传播和变化进行测量。将一个 TDR 连接到网络上，能够检测到未授权的获取网络数据的设备。

3. 查看进程

在 Windows 下，按 Ctrl＋Alt＋Del 组合键，查看"应用程序"、"进程"和"用户"项，若发现可疑的程序、进程和用户，则可怀疑机器被 sniffer，或是被病毒侵袭，或是正在被黑客攻击。

11.3.2　Sniffer 的防范措施

嗅探器通常是难以被发现的，因为它是被动的程序，一个老练的攻击者可以轻易通过破坏日志文件来掩盖信息，它们并不会给别人留下进行核查的尾巴。完全主动的解决方案很难找到，可以采用一些被动的防御措施。

- 安全的拓扑结构。
- 会话加密。
- 用静态的 ARP 或者 IP-MAC 对应表代替动态的 ARP。

1. 安全的拓扑结构

嗅探器只能在当前网段上进行数据捕获。这就意味着，将网络分段工作进行得越细，嗅探器能够收集的信息就越少。但是，除非用户的公司是一个 ISP，或者资源相对不受限制，否则这样的解决方案需要付出很大的代价。网络分段需要昂贵的硬件设备。有三种网络设备是嗅探器不可能跨过的，交换机、路由器和网桥。可以通过灵活的运用这些设备来进行网络分段。大多数早期建立的内部网络都使用 HUB 来连接多台工作站，这就是网络中数据的泛播（数据向所有工作站流通），让嗅探器能顺利地工作提供了便利。普通的嗅探器程序只是简单地进行数据的捕获，因此需要杜绝网络数据的泛播。随着交换机的价格下降，网络改造变得可行且很必要。不使用 HUB 而用交换机来连接网

络，就能有效地避免数据进行泛播，也就是避免让一个工作站接收与之不相关的数据。对网络进行分段，比如在交换机上设置 VLAN，使得网络隔离不必要的数据传送。一般可以采用 20 个工作站为一组，这是一个比较合理的数字。然后，每个月人为地对每个网段进行检测（也可以每个月采用 MD5 随机地对某个网段进行检测）。网络分段只适应于中小型的网络。如果有一个 500 个工作站的网络，分布在 50 个以上的部门中，若要对其完全分段的话，成本上是很高的。

2. 会话加密

会话加密提供了另外一种解决方案。不用特别地担心数据被嗅探，而是要想办法使得嗅探器不认识嗅探到的数据。这种方法的优点是明显的，即使攻击者嗅探到了数据，这些数据对他也是没有用的。S/key 和其他一次性口令技术一样，使窃听账号信息失去意义。S/key 的原理是远程主机已得到一个口令（这个口令不会在不安全的网络中传输），当用户连接时会获得一个“挑战”(challenge)信息，用户将这个信息和口令经过某种算法运算，产生正确的“响应”(response)信息（如果通信双方口令正确的话）。这种验证方式无须在网络中传输口令，而且相同的“挑战/响应”也不会出现两次。它的缺点是所有账号信息都存放在一台主机中，如果该主机被入侵，则会危及整个网络安全。另外配置它也不是一件简单的事情。Kerberos 包括流加密 rlogind 和流加密 telnetd 等，它可以防止入侵者捕获用户在登录完成后所进行的操作。在加密时有两个主要的问题：一个是技术问题，一个是人为问题。

技术问题是指加密能力是否高。例如，64 位的 DES 加密就可能不够安全，而且并不是所有的应用程序都集成了加密支持。另外，跨平台的加密方案还比较少见，一般只在一些特殊的应用之中才有。人为问题是指，有些用户可能不喜欢加密，他们觉得这太麻烦。用户可能开始会使用加密，但很少能够坚持下来。总之，必须寻找一种友好的媒介，还要具有一定的用户友好性。使用 secure shell、secure copy 或者 IPv6 协议都可以使信息安全的传输。传统的网络服务程序，SMTP、HTTP、FTP、POP3 和 Telnet 等在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，嗅探器非常容易就可以截获这些口令和数据。SSH 的英文全称是 Secure Shell。通过使用 SSH，用户可以把所有传输的数据进行加密。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、POP 甚至 PPP 提供一个安全的“通道”。SSH 绑定在端口 22 上，其连接采用协商方式使用 RSA 加密。身份鉴别完成之后，后面的所有流量都使用 IDEA 进行加密。SSH 程序可以通过网络登录到远程主机并执行命令。SSH 的加密隧道保护的只是中间传输的安全性，使得任何通常的嗅探工具软件无法获取发送的内容。它提供了很强的安全验证措施，可以在不安全的网络中进行安全的通信，所以它是防范嗅探器的一种较好的方法。

3. 用静态的 ARP 或者 IP-MAC 对应表代替动态的 ARP 或者 IP-MAC 对应表

该措施主要是进行渗透嗅探的防范，采用诸如 ARP 欺骗手段能够让入侵者在交换网络中顺利完成嗅探。网络管理员需要对各种欺骗手段进行深入了解，比如嗅探中通常

使用的 ARP 欺骗，主要是通过欺骗进行 ARP 动态缓存表的修改。在重要的主机或者工作站上设置静态的 ARP 对应表，比如 Windows 2000/XP 系统使用 ARP 命令设置，在交换机上设置静态的 IP-MAC 对应表等，防止利用欺骗手段进行嗅探的手法。

1）本机 MAC 地址和 IP 地址的查找

在 DOS 命令窗口下，用 ipconfig -all 命令查找本机的 MAC 地址和 IP 地址。如图 11-4 所示。



图 11-4　本机 MAC 地址及 IP 地址

2）ARP 命令的用法

```
ARP [-a] -s] -d] < IP Address> < MAC Address>
```

参数说明如下：

-a：显示 ARP 命令帮助。

-s：绑定一个 MAC 地址和 IP 地址。

-d：删除一个绑定。

例如：

```
arp -s 10.1.23.31 00-0E-A6-B4-32-84
```

习　题　11

1. 网络嗅探的基本原理是什么？
2. 网卡有哪几种数据接收模式？
3. 如何在网络上发现 Sniffer？
4. Sniffer 的防范措施有哪些？

第 12 章 chapter 12

病毒诊断与防治技术

12.1 计算机病毒概述

12.1.1 计算机病毒的定义

1. 病毒的定义

美国计算机研究专家 F. Cohen 博士最早提出了“计算机病毒”的概念，计算机病毒是一段人为编制的计算机程序代码。这段代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。其特性在很多方面与生物病毒有着极其相似的地方。

《中华人民共和国计算机信息系统安全保护条例》第二十八条中对计算机病毒做的定义是：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

广义上说，凡能够破坏计算机正常运行和破坏计算机中数据并能进行自我复制的程序代码都可以称为计算机病毒。

2. 计算机病毒的发展

从 1987 年发现第 1 例计算机病毒以来，计算机病毒的发展经历了以下几个主要阶段：DOS 引导阶段、DOS 可执行文件阶段、混合型阶段、伴随及批次性阶段、多形性阶段、生成器及变体机阶段、网络及蠕虫阶段、视窗阶段、宏病毒阶段和互联网病毒阶段。

12.1.2 计算机病毒的基本原理

1. 计算机病毒的工作原理

1）计算机病毒的主要特征

- 可控性。计算机病毒与各种应用程序一样也是人为编写出来的，是可控制的。
- 传染性。病毒的传染性又称“自我复制”或“再生”。再生是判断是不是计算机病毒的最重要依据。在一定条件下，病毒通过某种渠道从一个文件和一台计算机传

染到另外没有被病毒传染的文件和计算机。

- 夺取系统控制权。计算机病毒的首要目标就是争夺系统的控制权。一般采用修改中断入口或在正常程序中插入一段病毒程序,在系统启动或程序调用时,先运行病毒程序,而后才转向正常的系统或程序运行。
- 隐蔽性。计算机病毒的隐蔽性表现在两个方面:其一,传染的隐蔽性,大多数病毒在进行传染时不具有外部表现,不易被人发现;其二,一般的病毒程序都夹在正常程序之中,很难被发现。
- 潜伏性。一个编制精巧的计算机病毒程序,传染计算机或网络后,可以潜伏几周或者几个月甚至几年。

2)计算机病毒发作的触发条件

- 利用系统时钟提供的时间作为触发机制,这种触发机制被大量病毒使用。如CIH病毒是在每月的26日才会触发,“黑色星期五”病毒是在既是13日又是星期五的日子才触发。
- 利用病毒体自带的计数器作为触发器。
- 利用特定环境作为触发条件。

3)不可预见性

不同种类病毒的代码千差万别,病毒的制作技术也在不断地提高,病毒相对于反病毒软件永远是超前的。新的操作系统和应用系统的出现,软件技术不断地发展,这在为计算机提供了新的发展空间的同时,也使未来病毒的预测更加困难,这就要求人们不断提高对病毒的认识,增强防范意识。

4)病毒的衍生性、持久性和欺骗性

- 人们可以对一种计算机病毒进行改进,从而衍生出一种不同于原版本的新的计算机病毒(又称为变种病毒)。
- 计算机病毒程序可由一个受感染的备份通过网络系统反复传播,使得病毒的感染具有持久性和复杂性。
- 计算机病毒行动诡秘,而计算机对其反应却较“迟钝”,往往把病毒造成的错误当成事实接受下来,这就是计算机病毒的欺骗性。

2. 计算机病毒的作用机理

任何一种计算机病毒都是由引导、传染和表现3个部分组成的。

- 病毒的引导部分的作用是将病毒的主体加载到计算机内存,为感染部分作准备,在这期间发生驻留内存、修改中断地址、修改存放在高端内存中的信息、保存原中断向量等操作。引导部分也就是病毒的初始化部分,它随着宿主程序的执行而进入内存,为传染部分做准备。
- 病毒的传染部分的作用是将病毒代码程序自动传染到目标上去。不同的病毒在传染方式和传染条件上各有不同。
- 病毒的表现部分是病毒主体部分,病毒对计算机系统的破坏就是表现部分的作为,病毒的引导部分及传染部分都是为表现部分服务的。大部分病毒都是在一定

的条件下才会触发其表现部分的。

12.1.3 计算机病毒的分类

1．DOS 病毒（DOS virus）

指针对 DOS 操作系统开发的病毒。由于 Windows 2000/XP/2003 病毒的出现，DOS 病毒几乎绝迹。但 DOS 病毒在 Windows 2000/XP/2003 环境中仍可以进行感染，因此若执行了染毒程序，Windows 2000/XP/2003 用户也会被感染。使用现代的杀毒软件能够查杀的病毒中一半以上都是 DOS 病毒，可见 DOS 时代 DOS 病毒的泛滥程度。但这些众多的病毒中除了少数几个让用户胆战心惊外，大部分病毒都只是制作者出于好奇或对公开代码进行一定变形而制作的病毒。

2．Windows 病毒（Windows virus）

主要指针对 Windows 2000/XP/2003 操作系统的病毒。现在的计算机用户一般都安装 Windows 系统，Windows 病毒一般感染 Windows 2000/XP/2003 系统，其中最典型的病毒是 CIH 病毒。但这并不意味着可以忽略系统是 Windows NT 系列包括 Windows 2000/XP/2003 的计算机。一些 Windows 病毒不仅在 Windows 2000/XP/2003 上正常感染，还可以感染 Windows NT 上的其他文件。主要感染的文件扩展名为 EXE、SCR、DLL 和 OCX 等。

3．入侵型病毒（intrusion virus）

可用自身代替正常程序中的部分模块或堆栈区。因此这类病毒只攻击某些特定程序，针对性强。一般情况下难以发现，清除起来较困难。

4．嵌入式病毒（embedded virus）

这种病毒将自身代码嵌入到被感染文件中，当文件被感染后，查杀和清除病毒都很困难。由于编写嵌入式病毒比较困难，所以这种病毒数量不多。

5．外壳类病毒（shell virus）

这种病毒将自身代码附着于正常程序的首部或尾部。该类病毒的种类繁多，大多感染文件的病毒都是这种类型。

6．引导区病毒（boot virus）

通过感染软盘的引导扇区和硬盘的引导扇区或者主引导记录进行传播的病毒。

7．文件型病毒（file virus）

指将自身代码插入到可执行文件内来进行传播并伺机进行破坏的病毒。

8. 宏病毒(macro virus)

使用宏语言编写,可以在一些数据处理系统(主要是微软的办公软件系统、字处理、电子数据表和其他 Office 程序中)中运行,利用宏语言的功能将自己复制并且繁殖到其他数据文档里的程序。

9. 蠕虫病毒(worm virus)

通过网络或者程序漏洞自主传播,向外发送带毒邮件或通过即时通信工具(QQ、MSN 等)发送带毒文件,阻塞网络的正常通信。

10. 特洛伊木马(Trojan)

通常假扮成有用的程序诱骗用户主动激活,或利用系统漏洞侵入用户计算机。木马进入用户计算机后隐藏在的系统目录下,然后修改注册表,完成黑客定制的操作。

11. 后门程序(backdoor)

会通过网络或者系统漏洞进入用户的计算机并隐藏在系统目录下,被开后门的计算机可以被黑客远程控制。黑客可以用大量被植入后门程序的计算机组成僵尸网络(Botnet)用以发动网络攻击等。

12. 恶意脚本(harm script)、恶意网页

使用脚本语言编写,嵌入在网页当中,调用系统程序、修改注册表对用户计算机进行破坏,或调用特殊指令下载并运行病毒、木马文件。

13. 恶意程序(harm program)

会对用户的计算机、文件进行破坏的程序,本身不会复制和传播。

14. 恶作剧程序(joke)

这一类程序不会对用户的计算机、文件造成破坏,但会降低计算机和网络的运行效率,并会给用户带来恐慌和不必要的麻烦。

12.1.4 计算机病毒的破坏能力

- 病毒激发对计算机数据信息的直接破坏作用。
- 干扰系统运行,使运行速度下降。
- 占有磁盘空间和对信息的破坏。
- 强占系统资源。
- 干扰 I/O 设备,篡改预定设置以及扰乱运行。
- 破坏网络系统,非法使用网络资源,破坏电子邮件,发送垃圾信息,占用网络带宽等。

12.2 计算机病毒的诊断与防治技术

12.2.1 计算机病毒的检测

1. 计算机病毒的表现

当一台计算机染上病毒之后，会有许多明显的特征。例如，文件的长度和日期忽然改变，系统执行速度下降，出现一些奇怪的信息，无故死机，更为严重的是硬盘已经被格式化了。

如果用户的计算机上出现下述现象，则有可能是感染了计算机病毒。

- 系统启动速度比平时慢。
- 系统运行速度异常。
- 某些文件的长度及文件的建立日期发生变化。
- 没有发出“写”操作命令而出现“磁盘写保护”的提示。
- 在内存中发现不明程序的驻留或不明进程的运行。
- 打印机、显示器有异常现象。
- 系统自动生成一些不明的特殊文件。
- 文件莫名奇妙地丢失。
- 系统自动关机。
- 系统经常异常死机。

2. 计算机病毒的诊断

常见的防毒软件是如何去诊断病毒的呢？就是利用所谓的病毒码(virus pattern)。

病毒码其实可以想象成是犯人的指纹，当防毒软件公司收集到一个新的病毒时，就会从这个病毒程序中，截取小段独一无二足以表示这个病毒的二进制程序代码(binary code)，来当作扫毒程序辨认病毒的依据，而这段独一无二的二进制程序码就是所谓的病毒码。

反病毒软件常用以下 6 种技术来查找病毒。

1）病毒码扫描法

将新发现的病毒加以分析，根据其特征，编成病毒码，加入资料库中。以后每当执行扫描病毒程序时，能立刻扫描目标文件，并与病毒代码对比，即能侦察到是否有病毒。大多数防毒软件均采用这种方式，其缺点是无法扫描新病毒及变种病毒。

2）加总比对法

根据每个程序的文件名称、大小、时间及内容，加总(按位加)为一个检查码，再将检查码附于程序的后面或是将所有检查码放在同一个资料库中，利用加总法追踪并记录每个程序的检查码是否遭到更改，以判断是否中毒。这种技术可侦察到各种病毒，但最大的缺点是误判较高，且无法确认是哪种病毒感染的。

3）人工智能陷阱

人工智能陷阱是一种监测计算机行为的常驻内存扫描技术。它将所有病毒所产生的行为归纳起来，一旦发现内存的程序有任何不当的行为，系统就会有所警觉。这种技术的优点是执行速度快，且可以侦察到各种病毒；其缺点是程序设计难度大。

4）软件模拟扫描法

软件模拟扫描技术专门用来对付“千面人”病毒(polymorphic/mutation virus)。千面人病毒在每次传染时，都以不同的随机乱数加密于每个中毒文件中，传统病毒码比对方式根本就无法找到这种病毒。

5）先知扫描法

软件模拟技术可以建立一个保护模式下的DOS虚拟机器，模拟CPU动作并通过执行程序以解开变体引擎病毒，类似的技术也可以用来分析一般程序检查可疑的病毒码。因此，VICE可用来判断程序有无病毒码存在的方法，分析专家系统知识库，再利用软件工程模拟技术(software emulation)加上病毒运行机制，则可分析出新的病毒码以对付以后的病毒。这就是先知扫描法VICE(Virus Instruction Code Emulation)。

6）实时I/O扫描

实时I/O扫描(real_time I/O scan)的目的是在于及时地对数据的输入输出动作做病毒码对比，希望能够在病毒尚未被执行之前，就能够截留下来。实时扫描技术会影响到数据的输入输出速度，但使用实时扫描技术后，文件一旦传入就已经被扫描和清除过病毒了。

1222 计算机病毒的防范措施

防范网络病毒的过程实际上就是技术对抗的过程，反病毒技术也得适应病毒繁衍且随其传播方式的发展而不断调整。

1. 系统防毒措施

- 制定系统的防毒策略。
- 部署多层防御策略。
- 定期更新防毒定义文件和引擎。
- 定期备份文件。
- 预订可发布新病毒威胁警告的电子邮件。

2. 终端用户防毒措施

- 对于来历不明的邮件，最好不要轻易打开而是将其直接删除。
- 如果将Microsoft Word当作电子编辑使用，就需要将NORMAL.DOT在操作系统级设置只读文件。同时将Microsoft Word的设置更改为“Prompt to Save Normal Template(保存常规模板)”。许多病毒通过更改NORMAL.DOT文件进行自我传播，采取上述措施可产生阻止作用。
- 加上存储介质的写保护功能。

3. 服务器防毒措施

目前随着基于 Web 的电子邮件访问,公共文件夹以及访问存储器的映射网络驱动器等方式的出现,病毒也可以通过多种方式进入电子邮件服务器。这时,就只有基于电子邮件服务器的解决方案才能检测和删除受感染的文件。从以下几个方面可以做到防毒:

- 拦截受感染的附件。
- 设置全面的随机扫描。
- 试探随机扫描。
- 重要数据定期保存、备份。

4. 多层防御机制

多层防御体系将病毒检测、多层数据保护和集中式管理集成起来,提供全面的病毒防护能力,从而达到"治疗"病毒的效果。病毒检测一直是病毒防护的支柱,多层次防御软件使用了 3 层保护功能,实时扫描、完整性保护和完整性检验。

- 后台实时扫描驱动器能对未知的异形病毒和秘密病毒进行连续的检测。
- 完整性保护可阻止病毒从一个感染的工作站扩散到服务器,还可以防止与未知的病毒感染有关的文件崩溃。
- 完整性检验无需冗余的扫描而提高实时检验的性能。

5. 在网关、服务器上防御措施

防范手段应集中在网络整体上,在个人计算机的硬件和软件、LAN 服务器、服务器上的网关、Internet 及 Internet 的网站上,应层层设防,对每种病毒都实行隔离、过滤。

12.3 网络病毒的诊断与防治

12.3.1 网络病毒的特征

网络病毒是一种新型病毒,它的传播媒介不再是移动式载体,而是网络通道,这种病毒的传染能力更强,破坏力更大。有调查显示,通过电子邮件和网络进行病毒传播的比例正逐步攀升,给人们的工作和生活带来了很多麻烦。因此有必要了解网络病毒的知识及特点,并对其采取相应的措施,以减少被网络病毒感染的侵袭和破坏。

1. 网络病毒的传播方式

网络病毒一般会试图通过以下 4 种不同的方式进行传播。

1) 邮件附件

病毒经常会附在邮件的附件里,起一个吸引人的名字,诱惑人们去打开附件,一旦人们打开附件,计算机就会感染上其中所附带的病毒。

2）E-mail

有些蠕虫病毒会利用 Microsoft Security Bulletin 的安全漏洞将自身藏在邮件中，并向其他用户发送一个病毒副本进行传播。正如在公告中所描述的那样，该漏洞存在于 Internet Explorer 之中，可以通过 E-mail 的附件来传染病毒，用户只要打开邮件就会使计算机感染上病毒，并不需要打开邮件附件。

3）Web 服务器

有些网络病毒攻击 IIS 4.0 和 5.0 Web 服务器。以"尼姆达"病毒为例，主要通过两种手段进行攻击。第一，它检查计算机是否已经被"红色代码Ⅱ"病毒所破坏，因为红色代码Ⅱ病毒会创建一个"后门"，任何恶意用户都可以利用这个"后门"获得对系统的控制权。如果"尼姆达"病毒发现了具有这种"后门"的计算机后，就会利用"红色代码Ⅱ"病毒留下的后门来感染计算机。第二，病毒会试图利用"Web Server Folder Traversal"漏洞来感染机器。

4）文件共享

还有一种病毒的传播手段是通过文件共享来进行的。Windows 系统可以被配置成允许其他用户读写系统中的文件，之后允许所有人访问系统中的文件。如果病毒发现系统被配置为其他用户有创建文件的权限时，将会在该系统中添加文件来传播病毒。

2. 网络病毒的特点

1）感染速度快

在单机环境下，病毒只能通过软盘从一台计算机带到另一台，而在网络中则可以通过网络通信机制迅速扩散。根据测定，对于一个局域网络在正常情况下，只要有一台工作站有病毒，就可在几十分钟内将网上的数百台甚至上千台计算机全部感染。

2）扩散面广

由于病毒在网络中扩散非常快，扩散范围很广，不但能迅速传染局域网内所有计算机，还能通过远程工作站将病毒在一瞬间传播到千里之外。

3）传播的形式复杂多样

计算机病毒在网络上一般是通过"工作站/服务器/工作站"的途径进行传播的，但传播的形式复杂多样。

4）通过工作站传染

病毒先传染工作站，在工作站内存驻留，当已感染病毒的工作站连入网络时再传染给服务器。

5）通过服务器感染

如果远程工作站被病毒侵入，病毒也可以通过数据交换进入网络服务器中，一旦病毒进入文件服务器，就可通过它迅速传染到整个网络的每一个计算机上。而对于无盘工作站来说，由于其并非真的"无盘"（它的盘是网络盘），当其运行网络盘上的一个带毒程序时，便将内存中的病毒传染给该程序或通过映像路径传染到服务器的其他文件上，因此无盘工作站也是病毒孳生的温床。

6）难以彻底清除

单机上的计算机病毒有时可通过删除带毒文件或低级格式化硬盘等措施将病毒彻底清除，而网络中只要有一台工作站未能消毒干净就可使整个网络重新被病毒感染，甚至刚刚完成清除工作的一台工作站就有可能被网上另一台带毒工作站所感染。因此，仅对工作站进行病毒清除，并不能解决病毒对网络的危害。

7）破坏性大

网络上病毒将直接影响网络的工作，轻则降低速度，影响工作效率，重则使网络崩溃，破坏服务器信息，使多年工作毁于一旦。

8）可激发性

网络病毒激发的条件多样化，可以是内部时钟、系统的日期和用户名，也可以是网络的一次通信。一个病毒程序可以按照病毒设计者的要求，在某个工作站上激发并发出攻击。

9）潜在性

网络一旦感染了病毒，即使病毒已被清除，其潜在的危险性也是巨大的。根据统计，病毒在网络上被清除后，85%的网络在30天内会被再次感染。

例如尼姆达病毒，会搜索本地网络的文件共享，无论是文件服务器还是终端客户机，一旦找到，便安装一个隐藏文件（名为Riched20.DLL）到每一个包含doc和eml文件的目录中，当用户通过Word、写字板、Outlook打开doc和eml文档时，这些应用程序将执行Riched20.DLL文件，从而使机器被感染，同时该病毒还可以感染远程服务器被启动的文件。带有尼姆达病毒的电子邮件，不需要打开附件，只要阅读或预览了带病毒的邮件，就会继续发送带毒邮件给通信簿里的其他人。

12.3.2 网络病毒的诊断技术

在防范网络病毒时，需要注意以下几点。

1. 留心邮件的附件

对于邮件附件尽可能小心，安装一套杀毒软件，在打开邮件之前对附件进行预扫描。因为有的病毒邮件恶毒之极，只要将鼠标移至邮件上，即使没有打开它，也会自动执行和感染。更不要打开陌生人来信中的附件文件，当收到陌生人寄来的一些自称是“不可不看”的附件时，千万不要贸然打开它，尤其对于一些“.exe”之类的可执行程序文件，更要慎之又慎！

2. 注意文件扩展名

因为Windows允许用户在文件命名时使用多个扩展名，而许多电子邮件程序只显示第一个扩展名，有时会造成一些假象。所以可以在“文件夹选项”中，设置显示文件名的扩展名，这样一些有害文件，如VBS文件就会原形毕露。注意，千万别打开扩展名为vbs、shs和pif的邮件附件，因为一般情况下，这些扩展名的文件几乎不会在正常附件中使用，但它们经常被病毒和蠕虫使用。例如，看到的邮件附件名称是wow.jpg，而它的全名实际是wow.jpg.vbs，打开这个附件意味着运行一个恶意的VBScript病毒，而不是jpg查看器。

3. 不要轻易运行来历不明的程序

对于一般人寄来的程序，都不要运行，就算是比较熟悉、了解的朋友们寄来的信件，如果其信中夹带了程序附件，但是他却没有在信中提及或是说明，也不要轻易运行。因为有些病毒是偷偷地附着上去的(也许朋友的计算机已经感染了病毒)，可他自己却不知道。比如 happy 99 就是这样的病毒，它会自我复制，跟着用户的邮件走。当收到邮件广告或者主动提供的电子邮件时，也不要打开附件以及它提供的链接。

4. 不要盲目转发信件

收到自认为有趣的邮件时，不要盲目转发，因为这样会帮助病毒传播；给别人发送程序文件甚至包括电子贺卡时，一定要先在自己的计算机中试试，确认没有问题后再发，以免好心办了坏事。

5. 堵住系统漏洞

现在很多网络病毒都是利用了微软的 IE 和 Outlook 的漏洞进行传播的，因此需要特别注意微软网站提供的补丁，可以通过下载和安装补丁文件或安装软件的升级版本来消除和阻止很多网络病毒。同时，及时给系统打补丁也是一个良好的习惯，可以让用户的系统时时处于最新、最安全的状态。要注意应该从信任度高的网站下载补丁。

6. 禁止 Windows Scripting Host

对于通过脚本“工作”的病毒，可以采用在浏览器中禁止 Java 或 ActiveX 运行的方法来阻止病毒的发作。禁用 Windows Scripting Host。Windows Scripting Host(WSH)运行各种类型的文本，但基本都是 VBScript 或 JScript。许多病毒和蠕虫，如 Bubbleboy 和 KAK. worm 使用 Windows Scripting Host，无须用户单击附件，就可自动打开一个被感染的附件，同时应该把浏览器的隐私设置设为“高”。

7. 不要随便接收附件

尽量不要从在线聊天系统的陌生人那里接收附件，比如 ICQ 或 QQ 中传来的东西。有些人通过在 QQ 聊天中取得对用户的信任之后，给用户发一些附有病毒的文件，所以对附件中的文件不要打开，先保存在特定目录中，然后用杀毒软件进行检查，确认无病毒后再打开。

8. 从正规网站下载软件

不要从任何不可靠的渠道下载任何软件，因为通常无法判断什么是不可靠的渠道，所以比较保险的办法是对安全下载的软件在安装前先做病毒扫描。

9. 多做自动病毒检查

用户应确保自己的计算机对插入的软盘、光盘和其他的可插拔介质，以及对电子邮

件和互联网文件都会做自动的病毒检查。

10. 使用最新杀毒软件

要养成用最新杀毒软件及时查毒的好习惯。但是千万不要以为安装了杀毒软件就可以高枕无忧了,一定要及时更新病毒库,否则杀毒软件就会形同虚设;另外,要正确设置杀毒软件的各项功能,充分发挥它的功效。

12.3.3 局域网病毒的防范技术

计算机病毒在网络中泛滥已久,而且在局域网中也能快速繁殖,导致局域网计算机的相互感染,下面介绍有关局域网病毒的防范技术。

个人用户感染病毒后,使用单机版杀毒软件即可清除,然而企业的网络中,一台机器一旦感染“尼姆达”病毒,病毒便会自动复制、发送并采用各种手段不停交叉感染局域网内的其他用户。

计算机病毒形式及传播途径日趋多样化,因此,大型局域网络系统的防病毒工作已不再像单台计算机病毒的检测及清除那样简单,需要建立多层次的、立体的病毒防护体系,而且要具备完善的管理系统来设置和维护对病毒的防护策略。

一个网络的防病毒体系是建立在每个局域网的防病毒系统上的,应该根据每个局域网的防病毒要求,建立局域网防病毒控制系统,分别设置有针对性的防病毒策略。

1. 增加安全意识

杜绝病毒,主观能动性起到很重要的作用。要从加强安全意识着手,对日常工作中隐藏的病毒危害增加警觉性,如安装一种大众认可的网络版杀毒软件,定时更新病毒版本,对来历不明的文件运行前进行查杀,每周查杀一次病毒,减少共享文件夹的数量,文件共享的时候尽量控制权限和增加密码等,都可以很好地防止病毒在网络中的传播。

2. 小心邮件

随着网络的普及,电子信箱成了人们工作中不可缺少的媒介。它方便快捷,在提高了人们的工作效率的同时,也无意之中成为了病毒的帮凶。有数据显示,如今有超过一半以上的病毒通过邮件进行传播。

尽管这些病毒的传播原理很简单,但由于人们的粗心和不重视,致使这类病毒传染得很快很广。例如,若所有的 Windows 用户都关闭了 VB 脚本功能,像“库尔尼科娃”这样的病毒就不可能传播。只要用户随时小心警惕,不要打开值得怀疑的邮件和邮件附件,就可把病毒拒绝在外。

3. 挑选网络版杀毒软件

选择一个功力高深的网络版病毒“杀手”是至关重要的。一般而言,查杀是否彻底,界面是否友好、方便,能否实现远程控制、集中管理是决定一个网络杀毒软件的三大要素。

12.4 常用病毒防护软件的使用技术

目前，计算机病毒防护软件很多，如金山毒霸、江民杀毒软件、瑞星反病毒软件、光华反病毒软件及诺顿(Norton AntiVirus)防病毒软件等。由于篇幅所限，本书只对“金山毒霸”和“Norton AntiVirus 防病毒软件”进行介绍。

12.4.1 金山毒霸

1. 金山毒霸简介

本小节以最新版本“金山毒霸 2007”为蓝本，介绍金山毒霸软件的查毒、杀毒和防毒技术。

金山毒霸 2007 是一款功能强大、方便易用的个人及家庭首选反病毒产品，包括金山毒霸、金山网镖、金山反间谍和金山漏洞修复 4 个组件。它能保护用户的计算机免受病毒、黑客、垃圾邮件、木马和间谍软件的攻击。金山毒霸 2007 发布了金山毒霸脱壳引擎模块，大幅度增强对壳的支持，即大幅度地改善了金山毒霸对已知病毒加壳后的查杀能力。

金山毒霸 2007 具有下述特点。

1) 两大领先技术

- 数据流杀毒技术。基于传统的静态磁盘文件和狭义匹配技术，更进一步从网络和数据流入手，极大地提高了查杀木马及其变种的能力。
- 主动实时升级技术。当有最新的病毒库或者功能出现时，只要用户处于上网状态，无需做任何操作，毒霸可自动下载更新版本并自动进行安装，防止被新病毒感染和破坏。

2) 三大核心引擎

- 反间谍。可将驻留于内存及硬盘中的间谍软件和木马程序彻底清除，保护用户的系统安全。
- 反钓鱼。防止钓鱼网站、钓鱼邮件的攻击。用户访问钓鱼网站时金山毒霸会自动拦截，防止用户的账号密码等重要信息被盗。
- 主动漏洞修复。可扫描操作系统及各种应用软件的漏洞，当新的安全漏洞出现时金山毒霸 2007 会下载漏洞信息和补丁程序，经扫描程序检查后自动帮助用户进行修补。

3) 四大利器

- 迅速抢先。一旦木马或间谍软件试图通过邮件盗取银行账号、信用卡号和网游账号时，系统会自动报警并提示用户，防止数据被泄密。并能自动清理用户在计算机中留下的使用记录。
- 抢先加载。防毒胜于杀毒，抢先启动的防毒系统可保障在 Windows 未完全启动时就开始保护用户的计算机系统，早于绝大多数开机自运行的病毒程序，使用户

的计算机避免“带毒杀毒”的危险。抢先式防毒让计算机的安全也抢先了一步。

• 文件粉碎。“文件粉碎器”把用户要销毁的文件彻底删除。
• 应急 U 盘。支持创建应急杀毒 U 盘，在 Windows 系统不能正常启动的情况下，可以用应急 U 盘启动系统，自动查杀病毒并恢复系统。

在本小节中，介绍的是最新版的金山系统：金山毒霸 2007 版组合装。金山毒霸是一个套装软件，它包括了金山毒霸、金山反间谍、金山网镖和金山漏洞修复等 4 个组件，如图 12-1 所示。



图 12-1 金山毒霸 2007 套装软件主界面

2. “金山毒霸 2007”组件

利用“金山毒霸 2007”组件对计算机进行病毒的诊断、清除。金山毒霸组件操作窗口如图 12-2 所示。同时可对风险程序及携带病毒的文件给出详细的报告，如图 12-3 及图 12-4 所示。



图 12-2 金山毒霸组件



图 12-3　风险程序报告

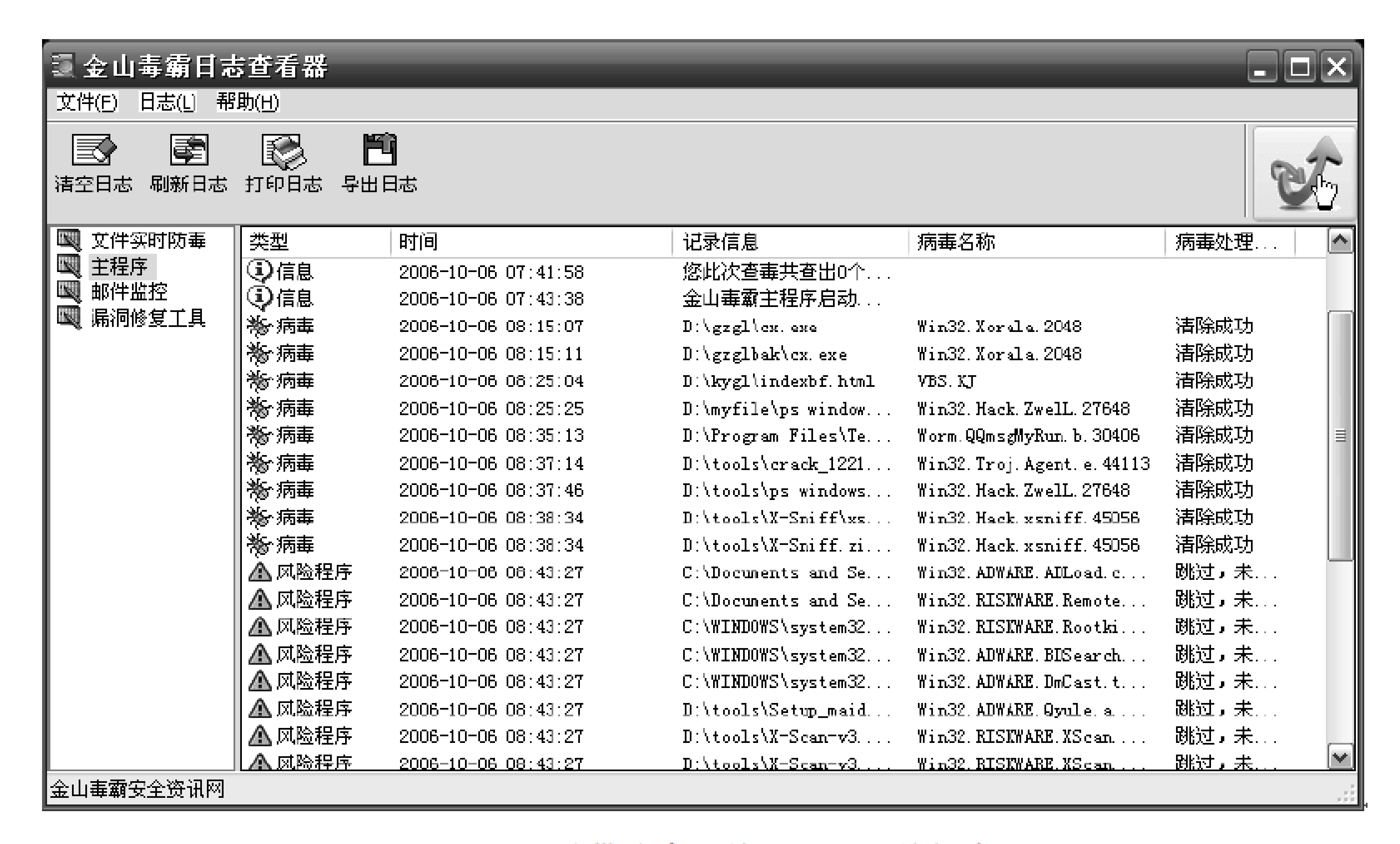


图 12-4　携带病毒文件及风险文件报告

3. “金山反间谍 2007”组件

利用“金山反间谍 2007”组件可以对计算机进行扫描，用以发现本机是否受到非法用户或非法进程的攻击。金山反间谍组件操作窗口如图 12-5 所示。

4. “金山网镖 2007”组件

利用“金山网镖 2007”组件，可对本机或网络进行实时监控，对非法进程和可疑进程进行拦截。金山网镖组件操作窗口如图 12-6 所示。



图 12-5 金山反间谍组件



图 12-6 金山网镖组件

金山网镖启动后，自动对计算机进行实时监控，对试图访问本机及时性局域网络的可疑进程进行拦截，并给出提示对话框，如图 12-7 所示。

管理员或操作员可根据实际情况对所拦截的进程放行或阻止。在图 12-7 中，单击"允许"按钮，则允许该进程访问本机及网络，若单击"禁止"按钮，则阻止该进程对本机或网络的访问。

5. "金山漏洞修复 2007"组件

"金山漏洞修复 2007"组件用以扫描本机或局域网络存在的安全漏洞，对本机上存在的安全漏洞可自动进行修复。金山漏洞修复组件操作窗口如图 12-8 所示。

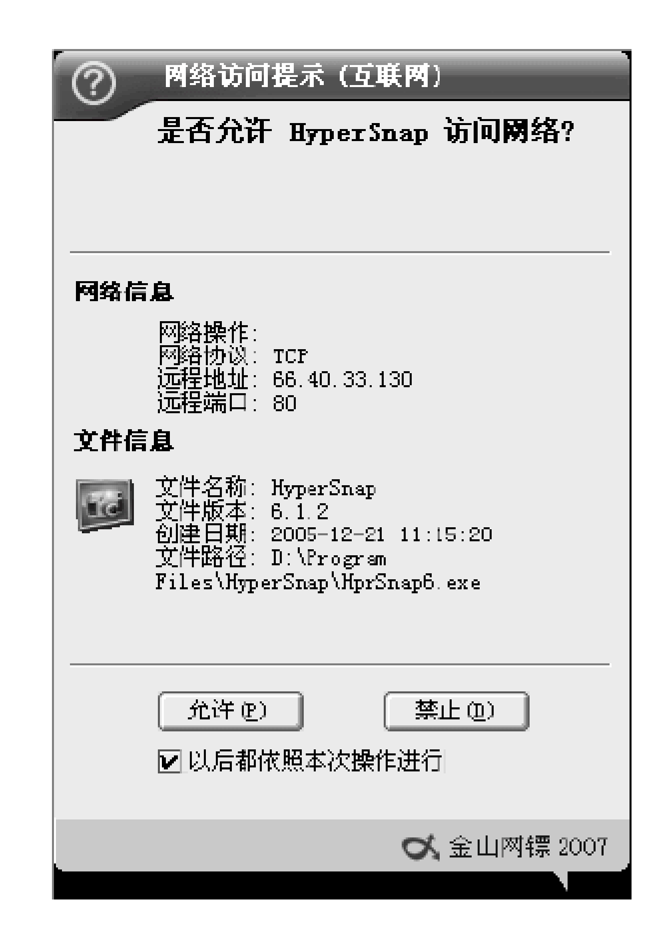


图 12-7　金山网镖对访问进程的拦截



图 12-8　金山漏洞修复组件

12.4.2　Norton AntiVirus 防病毒软件

1. Norton AntiVirus **软件简介**

Norton AntiVirus，中文简称诺顿防病毒软件，是最受信赖的防病毒软件之一。无论是在网上冲浪、聊天、发送电子邮件还是交换文件，Norton AntiVirus 诺顿防病毒都可以防御大量的互联网威胁。它可以自动检测并杀除病毒、除去计算机中不受欢迎的间谍软件，还可扫描电子邮件和附件的威胁，支持自动更新。

Symantec AntiVirus Corporate (Norton AntiVirus 诺顿杀毒软件企业版本)是世界上最优秀的杀毒软件之一，软件由 Symantec 公司开发，有企业版本、专业版本和标准版

本等，在这里介绍的是 Norton AntiVirus 企业版，与其他版本相比较，能为用户带来更低的系统资源占用，更可靠的性能。在本小节中介绍的是 Norton AntiVirus v9.0 版（软件下载网址 http://soft.mumayi.net/downinfo/3501.html，软件大小 18.26MB，软件运行环境 Windows 2000/XP）。

2. Norton AntiVirus v9.0 的安装

在 Norton AntiVirus v9.0 系统文件夹下，运行 Setup.exe 文件开始安装，当出现如图 12-9 所示的对话框时，根据本机的情况进行服务器和客户端的选择。若本机作为 Norton AntiVirus 服务器（可以监控一个局域网络），则选择“服务器安装”选项，若本机是一个客户端，则选择“客户端安装”选项。



图 12-9　客户端服务器选项

选择好安装选项后，单击“下一步”按钮，即往下安装。当出现如图 12-10 所示的对话框时，进行网络类型安装选择。



图 12-10　网络安装类型选择

网络安装类型选择完全由上一步的设置所定，若在“客户端服务器选项”对话框中选择了“服务器安装”选项，则在图 12-10 中选择“接受管理”，否则选择“不接受管理”，再单击“下一步”按钮。

之后，根据屏幕提示继续安装，当所有选择项选择完毕，即开始正式安装，如图 12-11 所示。



图 12-11　安装过程

3. Norton AntiVirus v9.0 的使用

1）软件的启动

单击“开始”|“所有程序”| Symantec Client Security-Symantec AntiVirus，启动 Norton AntiVirus v9.0，如图 12-12 所示。

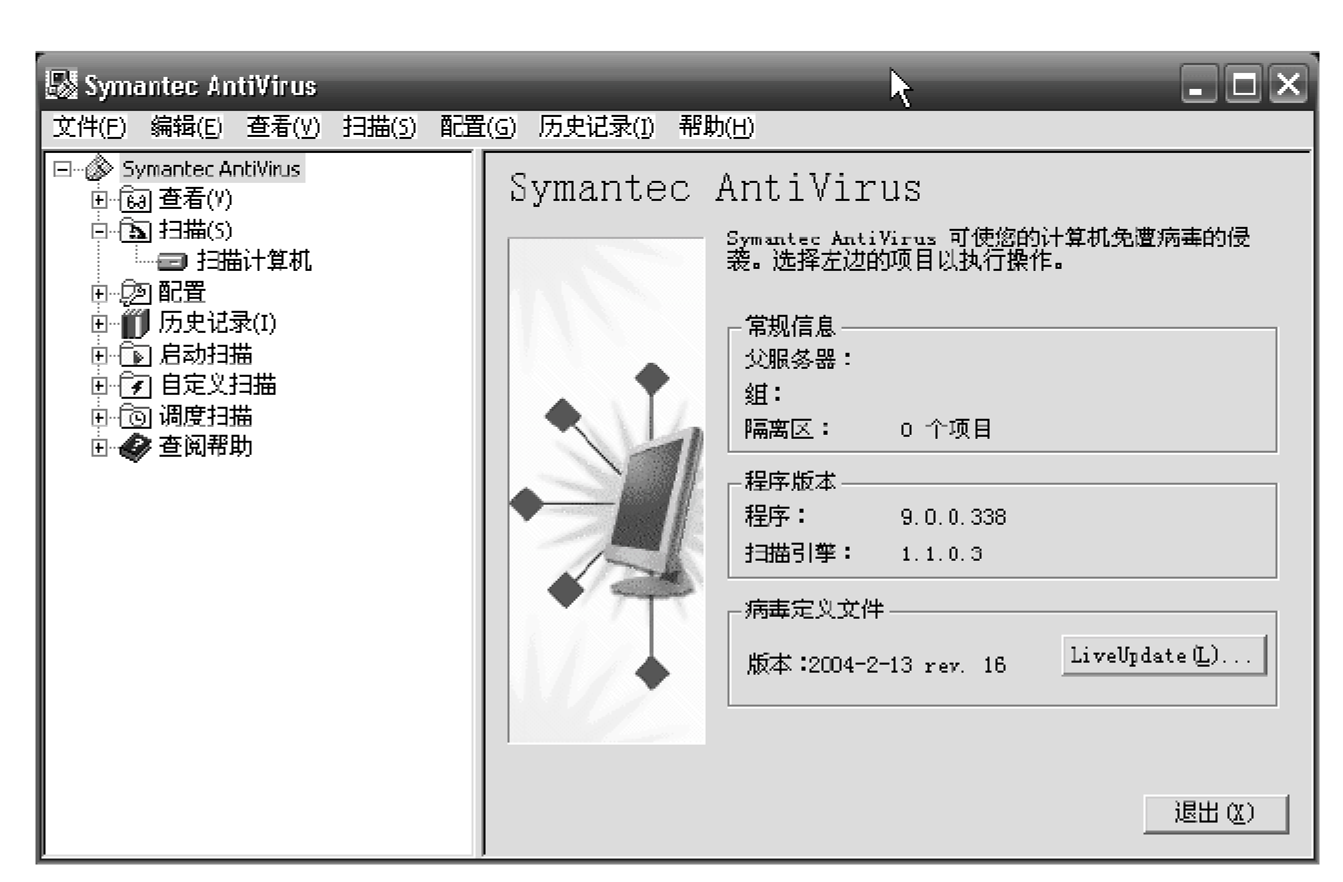


图 12-12　Norton AntiVirus v9.0 主窗口

2）扫描本地计算机

在图 12-12 所示的主窗口中，选择“扫描”|“扫描计算机”功能，得到本地计算机扫描窗口，如图 12-13 所示。

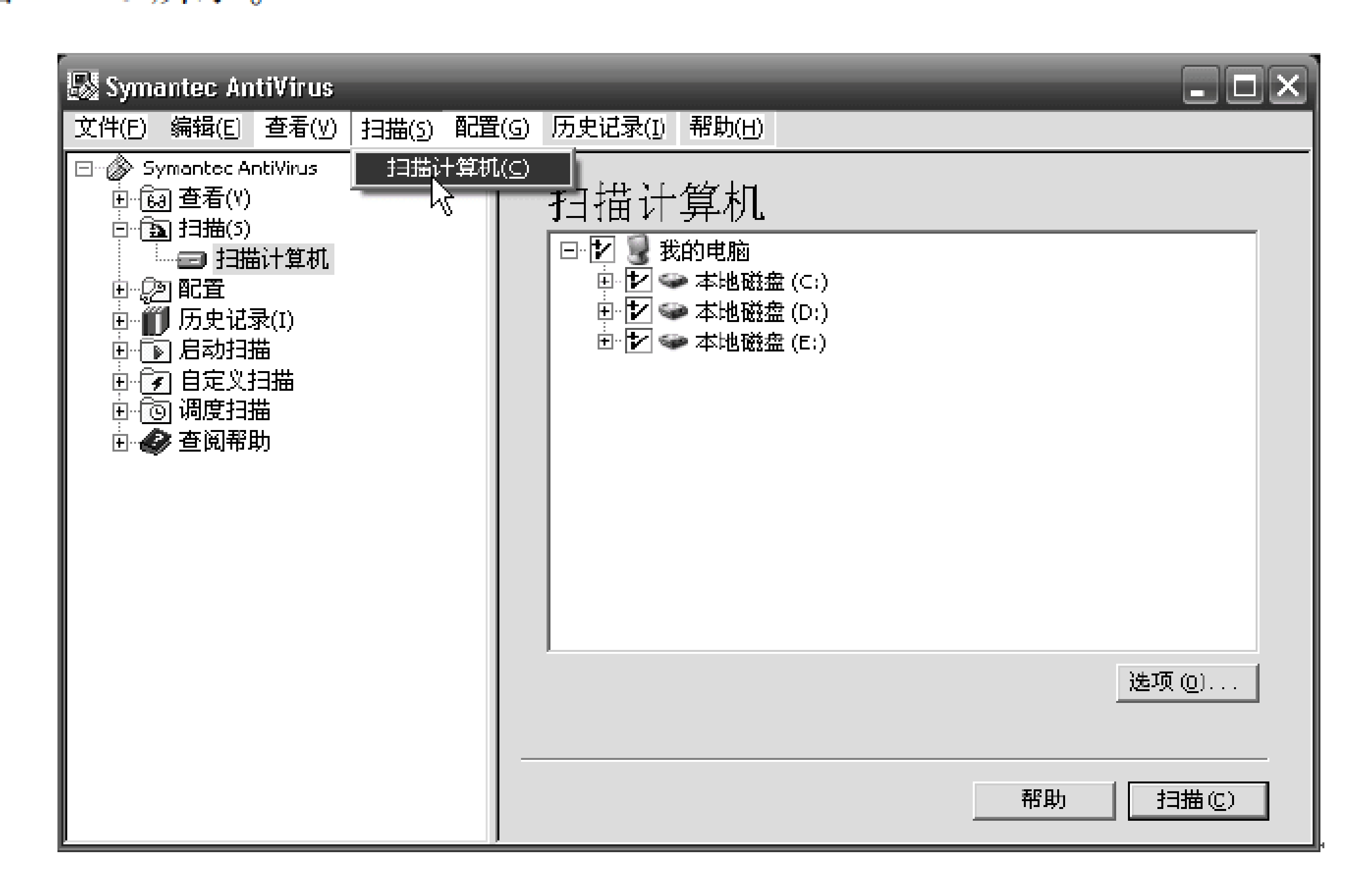


图 12-13 扫描本地计算机

在图 12-13 所示的窗口中，在右边“扫描计算机”窗口，选择所需扫描的磁盘，单击右下角的“扫描”按钮，即开始扫描本地计算机。

其他功能的操作使用根据屏幕提示即可。

12.5 应用实例

12.5.1 “震荡波”病毒的防范技术

2005 年 4 月底，反病毒专家们截获并消灭了专偷网上银行资金的病毒“网银大盗”病毒后，5 月 1 日，国家计算机病毒应急中心发现，一种利用微软操作系统漏洞的蠕虫病毒正在对互联网发起攻击，并陆续接到江苏、宁夏、北京、黑龙江、辽宁和广东等地区用户报告。凭着与计算机病毒多年的实战经验，专家们认为这个病毒潜在的危害巨大，病毒利用的是 Windows LSASS 的一个已知漏洞（MS04-011），被攻击的计算机会出现系统频繁重启的现象，与 2004 年大面积爆发的“冲击波”病毒危害十分相似。

通过对病毒样本的分析，该病毒特性如下：

- 该蠕虫不像往常的蠕虫那样通过邮件传播，而只是通过系统漏洞传播。
- 该蠕虫用来传播的文件名称是 avserve.exe（大小是 15 872B）。
- 该蠕虫的传播不需要人为的干预，该蠕虫能自动在网络上搜索含有漏洞的系统，引导这些有漏洞的系统下载病毒文件并执行。
- 病毒从 TCP 的 1068 端口开始搜寻可能的 IP 地址并试图传播。
- 病毒在 TCP 端口 5554，建立 FTP 文件服务器，该蠕虫能自动创建 FTP 脚本文件，并运行该脚本。该脚本能自动引导被感染的计算机下载病毒文件并执行。

一套完整的“震荡波”解决方案分为3步，称为“震荡波”完全解决3部曲：

第1步，针对病毒利用的是微软操作系统的已知漏洞MS04-011，解决的方法就是打上这个漏洞的补丁。下载地址为http://www.jiangmin.comexec/news_sys/news/jiangmin/index/important/2004511533255.htm。

第2步，对于已感染该病毒的用户，可用KV2004以上版本杀毒。

第3步，由于病毒利用TCP455、9995、5554端口，利用自身的IP地址列表，对特定IP地址段可能存在的计算机进行漏洞扫描并试图传播病毒，所以只需将以上端口封住即可，一般用户可以使用Windows 2000以上操作系统自带的TCP/IP筛选功能进行封堵。

对于没有经过微软合法授权的计算机用户，由于微软不提供相应的技术支持，安装相应的漏洞补丁程序是很困难的。因此，解决病毒的办法只能有后两种，即安装杀毒软件和封堵相应的端口。

12.5.2 “宏”病毒的防护技术

宏病毒是专门攻击Word、Excel文档的病毒，计算机染上宏病毒后，Word文档可能打不开，或打开后是乱码。该病毒于1996年9月首次登陆我国，是一种传染性和破坏性都很强的计算机病毒。

预防宏病毒最简单而有效的方法是在Word 2000/XP中进行安全设置保护，Word 2000/XP提供了防“宏病毒”的功能，方法是单击“工具”|“宏”|“安全性”，选择“高”选项，这样，当前打开的文档所使用的模板就有了防止“自动宏”执行的功能，当以后使用这个模板的文档时，如打开的文件带有“自动宏”，Word 2000/XP将首先告诉用户打开的文档带有自动宏，并询问用户是否执行宏，选择“否”，待进入并打开文档后，再自动对文档进行“宏”检查。

12.5.3 “爱虫”病毒的清除技术

“爱虫”病毒是一种邮件病毒，如果用户收到这样的一封邮件，邮件主题为“I LOVE YOU(我爱你)”，邮件内容为“Kindly check the attached I LOVELETTER coming from me(请尽快查收来自我的邮件附件中的求爱信)”，附件文件名为“LOVE-LETTER-FOR-YOU.htm”。该封邮件就是典型的“爱虫”病毒源。

如果用户出于好奇而打开了该邮件的附件，则用户的计算机就会自动感染“爱虫”病毒，所以，当收到主题为“I LOVE YOU”的邮件时，请直接将其删除，绝不要去打开和阅读其附件。

“爱虫”病毒的清除技术。

如果用户的计算机中了“爱虫”病毒，请用下述方法进行清除。

(1) 首先运行regedit.exe(在“开始”|“运行”下运行)，找到并删除键值HKEY_CURRENT_USER\Software\Microsoft\Windows Script(Host)\Settings。

(2) 在HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Mail下，输入一个正确的主页地址。

（3）删除 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下的 MSKernel32 键值。

（4）将键值 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunService 下的 Win32DLL 删除，再到 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下，如果有 WIN-BUGSFIX 键值，就删除它。

（5）找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ex-plorer\Doc Find Spec MRU。在这个条目包含所有最近使用过的文件，一般可以删除。

（6）删除 c:\windows\system 或 c:\windows\system32 目录下 MSKernel32. vbs、LOVE-LE-TTER-FOR-YOU. HTM 和 LOVE-LETTER-FOR-YOU. TXT. vbs 三个文件。同时删除 Windows 目录下的 Win32DLL. vbs 文件。

“爱虫”病毒侵袭的文件类型有 vbs、vbe、js、jse、css、wsh、sct、hta、jpg 以及 jpeg。这些文件被感染后，有可能不能恢复，不得不删除它。注意，要删除所有硬盘和所有网络驱动器上的有关文件。

最后查找 WIN-BUGSFIX. exe 或 WIN_BUGSFIX-32. exe 以及 script. ini，还有可能是 winfat32. exe，这些文件都是可能存在的，如果这些文件存在就将其删除。

注意，上述文件删除后，还要将回收站清空。

习 题 12

1. 什么是计算机病毒？
2. 计算机病毒的主要特征是什么？
3. 计算机病毒的作用机理是什么？
4. 计算机病毒的诊断技术有哪些？
5. 计算机病毒的多层防御体系是什么？
6. 网络病毒的传播方式有哪几种？
7. 金山毒霸 2007 由哪些组件组成？

第 13 章 chapter 13

黑客攻击与防范技术

“病毒”和“黑客”已成为现代网络的两大“杀手”，人们已从过去的谈“毒”色变转变为谈“黑”色变，因此，研究黑客、防范黑客对网络的威胁和攻击，是当今网络安全的重要研究内容。

本章的目的是让读者了解黑客，以帮助读者识别黑客，预防黑客，而不是教读者怎样当黑客，更不是教读者怎样去攻击别人的计算机或网站。

13.1 黑客的基本概念

13.1.1 黑客是什么

随着计算机网络的普及和发展，“黑客”与“入侵者”这两个名词也越来越引起世人的关注。

1. 黑客与入侵者

“黑客”在英文里是 hacker，其原意指的是对于任何计算机操作系统的奥秘都有强烈兴趣的人。“黑客”大都是高级程序员，他们具有深厚操作系统和编程方面的知识，精通计算机硬件结构及软件的内核结构，熟悉计算机软件硬件系统中的漏洞及其原因所在，并在网络结构及其原理方面有着很深的造诣。他们不断追求更深的知识，并向世人展示他们的发现，与他人分享，没有破坏数据的企图。这是人们早期对“黑客”的认识与定义。可以说，真正的“黑客”是计算机和网络的“天才”。

与“黑客”相对立的是“入侵者”，“入侵者”在英文里是 cracker，指的是怀有不良企图、非法闯入甚至破坏远程计算机完整性的人。“入侵者”利用获得的非法访问权，破坏重要数据，拒绝合法用户服务请求，或为了自己的个人目的而制造麻烦。硬币有正反两面，黑客也有好坏之分。有协助人们研究系统安全和网络安全的“正面黑客”，还有为捍卫国家尊严、维护民族利益的“黑客”，比如“红客联盟”。但也有不少专门窥探他人隐私，非法篡改和破坏他人的程序和数据的“反面黑客”。现在，在人们眼中，“黑客”已成为“网络上捣乱分子”和“网络犯罪分子”的代名词，很大程度是因为这些人总是用“黑客”自我命名和自我辩护。

现在,有许多人经常把“黑客”与“入侵者”混淆。多年来,人们误用“黑客”这个名词来表达“入侵者”的意思。其实,他们之间有着本质的不同。

今天,“黑客”一词已被用于泛指那些专门利用计算机搞破坏或恶作剧的家伙。对这些人的正确英文叫法应是 Cracker,有人翻译成“骇客”。黑客和骇客根本的区别是,黑客是网络的建设者,而骇客是网络的破坏者。

为了与人们的习惯称呼保持一致,在本章后面所讨论的“黑客”泛指 Cracker(入侵者)。

2. 黑客的分类

1) 好奇型

许多少年黑客往往是这方面的代表,他们年龄不大,社会经验少,思想性格还不是很成熟,缺乏社会约束力,在充分自由的网络环境中无法辨别自己行为的正确性,凭一时的兴趣、好奇潜入一些不该进入的网站,甚至获取了高度机密的资料,更有甚者对网站或网络造成破坏,而他们的内心,实际上却是非常的单纯,不是好奇就是好玩而已。

2) 功利型

往往是指那些想在网络上一举成名者,他们专门选择一些比较著名的网站进行攻击,制造混乱,唯恐天下不乱,以便自己“乱世出英雄”,名扬天下。对于功利型黑客可以区分为求名与求利两种,求利又可分为利己与利人两种。前一种为了自己的某种利益,比如盗取银行账号与密码,窃取不义之财;后一种为某种利益,受他人指使,或为某种政治目的对别的网站进行攻击。

3) 仇恨型

这类人往往处于嫉妒心理或是因某网站对自己的利益造成某种损害或威胁而采取的攻击行动,造成别的网站无法访问或瘫痪。

4) 恶作剧型

或许幽默是人的天性,这类黑客的数量也许是最多的,也是最常见的。这种网络黑客喜爱进入他人的计算机和网站中,或增加一些内容,如加入一则笑话以娱乐人或自娱;或者进入他人网址,将他人主页上的资料、信息做些更改,如 1996 年 8 月 17 日,为了抗议“正派通信法案”(这一法案禁止在因特网上传播黄色图片和文字),一些黑客破坏了美国司法部的网页,把司法部长的照片换成了希特勒,并放上了 2 张极为淫秽的黄色照片,写上了许多抗议美国政府压制言论自由的口号。

5) 制造矛盾型

这种网络黑客进入他人网站后,或修改他人的电子函件,或修改他人的商业合同,或修改生产厂家的商品生产日期,或修改他人的订货数量、品种,从而使他人产生各种各样的矛盾或纠纷。甚至于还有些网络黑客破坏他人的商业交易,并借此机会了解双方商谈之协议价格,从而趁机渔利。

6) 杀手型

这种网络黑客就一点也不客气了。他们非法进入他人网站后,或者将他人的重要文件、资料全部删除,或者涂改、删除他人的重要电子函件(如商品订货单),或者将病毒载

入他人网络网站中,使其网络无法正常运行。他们每到一处,都搞得鸡犬不宁,引起一场灾难。

7) 政治型

由于某种政治利益的需要,一些国家和政府利用黑客侵入他人的网络,窃取国家和军事机密信息。

13.1.2 国内黑客的发展历史

因特网在中国的迅速发展也使国内的黑客逐渐成长起来。纵观中国黑客发展史,可以分为 3 个阶段。

1. 第 1 阶段,中国黑客的起源(1994—1996 年)

20 世纪 90 年代初,中国互联网处于刚刚开始发展的朦胧时期,也就是在这一年,中国互联网的大门终于面向公众开放了。但是在那个年代,计算机还是一件非常奢侈的电子用品,而互联网对于大众来说更是一个陌生的名词,人们只有在专业性极强的书刊中能够找到与网络相关的名词,而上网的群体也多数是科研人员和知识分子。各地计算机发烧友最大的乐趣就是 COPY 那些小游戏和 DOS 等软件类产品,盗版对人们来说还是一个陌生的名词,对于广大计算机用户来说,COPY 就是正版的一种传播方式。于是,最早的黑客或者说"窃客"诞生了。那个时候,一个全新的小软件就几乎是计算机的全部生命与理解,而对于这些窃客来说能够 COPY 到国外的最新产品是他们最大的荣幸,那一张张的小软盘中承载了中国黑客最初的梦想。

在那个中国网络最为朦胧的岁月里,大多数玩家操作着比 9600b/s 还小的雏猫,在最为原始的网络上"慢跑"。那不是现在传统意义上的 Internet,而是最为初级的 BBS 站点,以一种依靠拨电话号码直接连接到 BBS 服务器上的方式来进行交流。

时光转眼到了 1996 年,在中国网民的年代分类中,在 1996 年以前接触网络的人被称为中国的第一代网民,或许在这其中有些人从来没有接触过 Internet,所接触的最多也就是那种电话连接的 BBS,但是他们仍然无愧于中国第一代网民。1995—1996 年这一期间,中国各个大中城市的互联网信息港基本已经初具规模,中国国际互联网的第一代网管诞生,中国第一代的大众网民也开始走出 BBS,而融入这种天地更为广阔的 Internet。那两年是中国互联网初步成长的时期,也同样是中国软件业开始蓬勃发展的时期。中国网络人以自己的方式做着自己的梦,在这些人中很多是接触过早期 BBS 的网友,在他们看来,从 BBS 移师 Internet 只不过将自己的舞台扩大了一些,让自己的眼睛看得更多了一些。当然在那个阶段,除了窃客以外,电话飞客也曾出现在中国,但是由于程控交换机的出现,飞客很快的成为了历史。1996 年底,中国电信开始实行优惠上网政策,在此之后中国网络开始了真正步入百姓家庭的步伐。与此同时,中国黑客也在初具规模的互联网络中诞生和发展。

2. 第 2 阶段,中国黑客的成长(1997—1999 年)

1997 年在中国互联网发展史上应该是最为值得纪念的一年,而在中国黑客成长过程

中，那一时期也哺育了众多的初级黑客，互联网这一个名词也逐渐被大众接受，新的思想，新的观念也逐渐从网络中折射出来。在 1997 年初期，Yahoo 搜索引擎中只能够搜索出 7 个跟黑客相关的简体中文网页。而且网站中的内容多数是翻译或者重复国外相同网页的内容，很多没有实际意义。不过此时“黑客”这一个名词已经开始正式地深入广大网民之中，当时初级黑客所掌握的最高技术仅仅是使用邮箱炸弹，并且多数是国外的工具，完全没有自己的黑客武器，更不要说自己的精神领袖。那个时期世界上的黑客共同追随着一个精神领袖凯文·米特尼克，世界头号黑客。这位传奇性人物不单单领导着美国黑客的思想，也影响着中国初级黑客前进与探索的方向。

1998 年，正当国内开始轰轰烈烈地开展互联网大跃进活动的时期，在大洋彼岸的美国，一年一度的黑客大会上由一个名为“死牛崇拜”黑客小组公布了一款名叫 BO（Back Orifice）的黑客软件，并将源代码一起发布。这个软件掀起了全球性的计算机网络安全问题，并推进了“特洛伊木马”这种黑客软件的飞速发展。BO 公布后，透过刚刚兴起的互联网迅速传到了中国，当时很多网友就是使用这款软件开始了对黑客生涯的初恋。但是 BO 并没有在中国掀起浪潮，当然因素是多种多样的，比如网络尚在发展中，BO 为舶来品不方便中国网友使用等。但是 BO 没有辉煌的另一个主要原因是 CIH 病毒的诞生和大规模发作。这个有史以来第一个以感染主板 BIOS 为主要攻击目标的病毒给中国经济带来了巨大的损失。

1998 年给还处在发育期的中国黑客带来了太多的惊奇、恐惧、理想与动力。在 BO 诞生不久，中国黑客自己的特洛伊木马也诞生了，这就是网络间谍 NetSpy。但是 NetSpy 的诞生并没有给中国黑客的发展带来太大的震动，这一切都让 CIH 的光芒所掩盖了。少量的国产工具开始小范围流行于中国黑客之间。当大家正在为杀毒而忙得不可开交的时候，一次国际性事件掀起了中国黑客首次浪潮。

木马冰河是中国黑客史中必须提到的一个软件，它由中国安全程序员编写，软件人员在开发这个软件的最初版本的时候并没有考虑到它能够作为一个特洛伊木马来使用，但随后冰河疯狂流行于黑客手中，很多用户在不知不觉中被冰河控制。早期的冰河还不能算是一个好的木马软件，随后软件开发人员用了大量的时间对冰河进行代码重构，冰河 2.2 版本诞生了。新版本的冰河迅速被流传出去，并让大批初级黑客快速地步入黑客这扇大门。中国黑客软件的开发从此走向了新的纪元，再次之后，黑洞、网络神偷、灰鸽子、XSan、YAI 等众多优秀的国产黑客软件纷纷涌现，黑客也开始出现商业化迹象，由前“绿色兵团”成员组建的“中联绿盟”网络安全公司成立，正式开始了黑客向商业化迈进的脚步，中国黑客逐渐成长了起来。

3. 第 3 阶段，浮躁的欲望（从 2000 年开始）

2000 年成为了中国网络最为辉煌的一年，网吧也在全国各地蜂拥出现，上网的人群更比 20 世纪增加了一倍多。一时间“你上网了吗?”成为了流行问候语。与此同时中国的黑客队伍也在迅速扩大着，众多的黑客工具与软件使得进入黑客的门槛大大降低，黑客不再是网络高手的代名词，很多黑客很有可能就是一个嘴里叼着棒棒糖手里翻着小学课本的孩子。

2000 年,一个全新的概念“蓝客”问世了。这时国内的黑客基本分成 3 种类型。一种是以中国红客为代表,是爱国主义情结的黑客。另外一种是以蓝客为代表,他们热衷于纯粹的互联网安全技术,对于其他问题不关心的技术黑客。最后一种就是完全追求黑客原始本质精神,不关心政治,对技术进行疯狂追求的本色黑客。

2001 年 4 月 1 日,我国南海地区发生了“中美撞机事件”后,美国一个名为 PoizonBOx 黑客组织率先向我国的一些网站发起了恶意的进攻。中美黑客产生了一些小的摩擦。到了五一假期,许多中国黑客拿起了手中的武器,大规模地向美国网站展开进攻。

近几年中,中国黑客思想开始逐渐成熟,众多黑客纷纷再次回归技术,不再热衷于媒体的炒作。黑客道德与黑客文化的讨论和延伸也让中国黑客逐步地重返自然状态,致力于对网络安全技术的研究。

相对于现在的中国黑客现状来说,中国黑客针对商业犯罪的行为不多,报刊出现一些所谓的商业黑客犯罪行为,实际上多属采用物理手段,而非网络手段。尽管见诸报端的中国黑客行为多体现为某种程度上的爱国情绪的宣泄,但是黑客行为毕竟大部分是个人行为,如果不加引导,有发展成计算机网络犯罪的可能。但是客观地说,中国黑客行动对我国网络安全起到了启蒙作用,没有黑客,就没有网络安全这个概念。同时,一批黑客高手已转变为网络安全专家,他们发现安全漏洞,研发出众多安全技术和安全软件,对我国计算机网络的发展做出了贡献。

13.2 黑客常用的攻击手段

13.2.1 黑客攻击步骤

黑客攻击的基本步骤如下:

(1) 搜集信息。

(2) 实施入侵。

(3) 上传程序,下载数据。

(4) 利用一些方法来保持访问,如后门、特洛伊木马。

(5) 隐藏踪迹。

在攻击者对特定的网络资源进行攻击以前,他们需要了解将要攻击的环境,这需要搜集汇总各种与目标系统相关的信息,包括计算机数目、类型和操作系统等。踩点和扫描的目的都是进行信息的搜集。

攻击者搜集目标信息一般采用 7 个基本步骤,每一步均有可利用的工具,攻击者利用它们得到攻击目标所需要的信息。

(1) 找到初始信息。

(2) 找到网络的地址范围。

(3) 找到活动的计算机。

(4) 找到开放端口和入口点。

(5) 识别主机操作系统。

(6) 识别每个端口运行的是哪种服务。

(7) 画出网络拓扑图。

1. 找到初始信息

攻击者危害一台计算机需要有初始信息,比如一个 IP 地址或一个域名。然后根据已知的域名搜集该站点的有关信息。比如服务器的 IP 地址或者这个站点的工作人员名单、电话号码等信息,这些信息足够帮助发起一次成功的社会攻击。

搜集初始信息的一些方法包括:

1) 开放来源信息 (open source information)

在一些情况下,公司会在不知不觉中泄露大量信息。比如公司认为是一般的、可以公开的客户信息,都能被攻击者利用。这种信息一般称为开放来源信息。

开放来源信息是关于公司或者它的合作伙伴一般的、公开的信息,是任何人都能够得到的信息。这意味着存取或者分析这种信息比较容易,并且没有犯罪的因素,是合法的。这里列出几种获取信息的例子:

- 公司新闻信息。如某公司为展示其技术的先进性和能为客户提供最好的监控能力、容错能力、服务速度,往往会不经意间泄露了系统的操作平台、交换机型号及基本的线路连接。
- 公司员工信息。大多数公司网站上附有全体员工姓名及地址簿、电话号码等,在上面不仅能发现公司主管和财务总监人员,而且也能得到公司的机构设置信息,这些信息足以让攻击者发起一次社会攻击。
- 新闻组。现在越来越多的技术人员使用新闻组、论坛来帮助解决公司的问题,攻击者也可从中得到一些有用的信息,比如知道公司有什么设备,还可帮助他们揣测出技术支持人员的水平。

2) Whois

对于攻击者而言,任何有域名的公司必定会泄露某些信息。

攻击者会对一个域名执行 Whois 程序以找到附加的信息。UNIX 的大多数版本装有 Whois 程序,所以攻击者只需在终端窗口或者命令提示行下执行"whois <要攻击的域名>"命令就可以了。对于 Windows 操作系统,要执行 Whois 查找,需要一个工具,比如 sam spade。

通过查看 Whois 的输出,攻击者会得到一些非常有用的信息,比如一个物理地址、一些人名和电话号码。非常重要的是通过 Whois 可获得攻击域的主要服务器 IP 地址。

3) Nslookup

找到附加 IP 地址的一个方法是对一个特定域询问 DNS。这些域名服务器包括特定域的所有信息和链接到网络上所需的全部数据。

另一个得到 IP 地址的简单方法是 ping 域名。ping 一个域名时,程序做的第一件事情是设法把主机名解析为 IP 地址并输出到屏幕。攻击者得到网络的地址,能够把此网络当作初始攻击站点。

2. 找到网络的地址范围

当攻击者找到了部分计算机的 IP 地址后，下一步需要找出网络的地址范围或者子网掩码。

需要知道地址范围的主要原因是，保证攻击者能集中精力对付一个网络而不至于闯入其他网络。这样做有两个原因，第一，假设有地址 10.10.10.5，要扫描整个 A 类地址需要相当长的一段时间。如果正在跟踪的目标只是地址的一个小子集，就可节省很多时间；第二，一些公司有比其他公司更好的安全性，因此跟踪较大的地址空间增加了危险。比如攻击者可能会闯入一个具有良好安全性的公司，它便报告这次攻击并发出报警。

攻击者能用两种方法找到这一信息，较容易实现的方法是使用 ARIN(America Registry for Internet Numbers)Whois 搜索找到信息；困难的方法是使用 tranceroute 解析结果。

- ARIN 允许任何人搜索 Whois 数据库找到“网络上的定位信息、自治系统号码(ASN)、有关的网络句柄和其他有关的接触点(POC)。”基本上，常规的 Whois 会提供关于域名的信息。ARINWhois 允许询问 IP 地址，帮助找到关于子网地址和网络如何被分割的策略信息。
- 使用 traceroute 可以找到一个数据包通过网络的路径。因此利用这一信息，能决定主机是否在相同的网络上。

连接到 Internet 上的公司有一个外部服务器把网络连到 ISP 或者 Internet 上，所有去往公司的流量必须通过外部路由器，否则进入不了网络，因大多数公司有防火墙，所以 traceroute 输出的最后一跳是目的计算机，倒数第二跳是防火墙，倒数第三跳是外部路由器。通过相同外部路由器的所有计算机属于同一网络，通常也属于同一公司。因此攻击者通过 tranceroute 查看到达的各种 IP 地址，看这些机器是否通过相同的外部路由器，就知道它们是否属于同一网络。

3. 找到活动的机器

在知道了 IP 地址范围后，攻击者想知道哪些计算机是活动的，哪些是不活动的。公司里一天中不同的时间有不同的计算机在活动。一般攻击者在白天寻找活动的计算机，然后在深夜再次查找，他就能区分工作站和服务器。服务器会一直被使用，而工作站只在正常工作日是活动的，晚上经常是处于关闭状态。

- ping。使用 ping 可以找到网络上哪些计算机是活动的。
- Pingwar。ping 有一个缺点，一次只能 ping 一台计算机。攻击者希望同时 ping 多台计算机，看哪些有反应，这种技术一般称为 ping sweeping。Pingwar 就是一个这样的有用程序。
- Nmap。Nmap 也能用来确定哪些计算机是活动的。Nmap 是一个有多用途的工具，是一个端口扫描仪，但也能 ping sweeping 一个地址范围。

4. 找到开放端口和入口点

1) Port Scanners

为了确定系统中哪一个端口是开放的，攻击者会使用被称为端口扫描仪(port

scanner)的程序。端口扫描仪可以找出哪些端口是开放的。

端口扫描仪有两个关键特征：第一，它能一次扫描一个地址范围；第二，能设定程序扫描的端口范围(能扫描 1～65 535 的整个范围)。

目前流行的扫描类型有：

- TCP conntect 扫描；
- TCP SYN 扫描；
- FIN 扫描；
- ACK 扫描。

常用端口扫描程序有：

- ScanPort。在 Windows 环境下使用，是一款基础的端口扫描仪，能详细列出地址范围和扫描的端口地址范围。
- Nmap：在 UNIX 环境下推荐的端口扫描仪是 Nmap。Nmap 不仅是端口扫描仪，也是安全工具箱中必不可少的工具。

2) War Dialing

进入网络的另一个普通入口点是 modem(调制解调器)。用来找到网络上的 modem 的程序称为 war dialer。当提交了要扫描的开始电话号码或者号码范围，它就会拨叫每一个号码寻找 modem 回答，如果有 modem 回答了，就会自动记录下这一信息。

THC-SCAN 是常用的 war dialer 程序。

5. 识别主机操作系统

利用上面的技术，攻击者可掌握哪些计算机是活动的和哪些端口是开放的，更进一步的工作就是要识别每台主机运行哪种操作系统。

有一些探测远程主机并能确定在该主机上运行哪种操作系统的软件。这些程序通过向远程主机发送不平常的或者没有意义的数据包来完成。每一个操作系统对它们的处理方法都不同，攻击者通过解析输出，能够弄清自己正在访问的是什么类型的设备和在运行哪种操作系统。

- Queso。是最早实现这个功能的程序，Queso 目前能够鉴别出范围从 Microsoft 到 UNIX 和 Cisco 路由器的有 100 多种不同的设备。
- Nmap。具有和 Queso 相同的功能，可以说它是一个全能的工具。目前能检测出接近 400 种不同的设备。

6. 识别每个端口运行的是哪种服务

1) default port and OS

基于公有的配置和软件，攻击者能够比较准确地判断出每个端口在运行什么服务。例如，如果知道操作系统是 UNIX 和端口 25 是开放的，能判断出机器正在运行 Sendmail；如果操作系统是 Microsoft Windows NT 并且端口 25 是开放的，就能判断出正在运行 Exchange。

2）Telnet

Telnet 是安装在大多数操作系统中的一个程序，它能连接到目的计算机的特定端口上。攻击者使用这类程序连接到开放的端口上，大多数操作系统的默认安装显示了关于给定的端口在运行何种服务的标题信息。

3）Vulnerability Scanner

Vulnerability Scanner（弱点扫描器）是能被运行来对付一个站点的程序，它向黑客提供一张目标主机弱点的清单。

7. 画出网络拓扑图

进入这一阶段，攻击者得到了各种所需的信息，进一步的工作就是画出网络拓扑图使之能找出最好的入侵方法。攻击者可以使用 traceroute 命令或者 ping 命令来找到这个信息，也可以使用诸如 cheops 程序，自动地画出网络拓扑图。

经过一系列的前期准备，攻击者搜集了很多信息，并有了一张网络的详尽图，确切地知道每一台计算机正在使用的软件和版本，并掌握了系统中的一些弱点和漏洞。当拥有了这些信息后，网络实际上相当于已受到了攻击。因此，保证网络安全最首要的任务就是使攻击者尽量少地获得信息。

13.2.2 密码破解

密码与用户账户的有效利用是网络安全性最大的问题之一。本小节将研究密码破解技术：如何进行密码破解？攻击者是如何进入网络的？使用的工具以及抗击的方法是什么？

对公司或组织的计算机系统进行的攻击有多种形式，例如电子欺骗、smurf 攻击以及拒绝服务攻击。这些攻击被设计成破坏或中断运营系统的使用。本小节讨论一种广为流传的攻击形式，称为“密码破解”技术。所谓“密码破解”，实质上是指在使用或不使用工具的情况下渗透网络、系统或资源，以解锁用密码保护的资源，其主要技术如下：

1. 字典攻击（dictionary attack）

简单的字典攻击是闯入机器的最快方法。字典文件（一个充满字典文字的文本文件）被装入破解应用程序，它是根据由应用程序定位的用户账户运行的。因为大多数密码通常是简单的，所以运行字典攻击通常足以实现目的了。

2. 混合攻击（hybrid attack）

另一个攻击形式是混合攻击。混合攻击将数字和符号添加到文件名以成功破解密码。许多人只通过在当前密码后加一个数字来更改密码。其模式通常采用这一形式，第一个月的密码是 cat，第二个月的密码是 cat1，第三个月的密码是 cat2，以此类推。

3. 蛮力攻击（brute force attack）

蛮力攻击又称穷举攻击，是最全面的攻击形式，它通常需要很长的时间，这取决于密

码的复杂程度。根据密码的复杂程度,某些蛮力攻击可能花很长的时间(几天、几个星期甚至几个月)。

4. 专业工具

最常用的工具之一是 LophtCrack(即 LC4)。LophtCrack 是允许攻击者获取加密的 Windows NT/2000 密码并将它们转换成纯文本的一种工具。Windows NT/2000 密码是密码散列格式,如果没有诸如 LophtCrack 之类的工具就无法读取。它的工作方式是通过尝试每个可能的字母数字组合试图破解密码。

另一个常用的工具是协议分析器(又称为网络嗅探器,如 Sniffer Pro 或 Etherpeek),它能够捕获它所连接的网段上的每块数据。当以混杂方式运行这种工具时,它可以"嗅探出"该网段上发生的每件事,如用户登录和数据传输。这会严重地损害网络安全性,使攻击者捕获密码和敏感数据。

5. 内部攻击

内部攻击者是解密攻击最常见的方式,因为攻击者具有对组织系统的直接访问权限。

6. 外部攻击

外部攻击者是指那些穿过"深度防御"闯入用户网络系统的人。一种常见的外部攻击形式称为"网站涂改",这一攻击使用密码破解来渗透攻击者想破坏的系统。另一种密码破解攻击是攻击者尝试通过社会工程(social engineering)获取密码。社会工程是哄骗一个毫无疑虑的管理员向攻击者说出账户标识和密码的欺骗方法。

13.2.3 Web 攻击

由于 Web 服务器提供了几种不同的方式将请求转发给应用服务器,并将修改过的或新的网页发回给最终用户,这使得非法闯入网络变得更加容易。

而且,许多程序员不知道如何开发安全的应用程序。他们只会使用现成的 Intranet Web 应用程序,这些应用程序没有考虑到在安全缺陷被利用时可能会出现灾难性后果。

其次,许多 Web 应用程序容易受到通过服务器、应用程序和内部已开发的代码进行的攻击。这些攻击行动直接通过了周边防火墙安全措施,因为端口 80 或 443(SSL,安全套接字协议层)必须开放,以便让应用程序正常运行。Web 应用程序攻击包括对应用程序本身的 DoS(拒绝服务)攻击、改变网页内容以及盗走企业的关键信息或用户信息等。

总之,Web 应用攻击之所以与其他攻击不同,是因为它们很难被发现,而且可能来自任何在线用户,甚至是经过验证的用户。目前,企业用户主要使用防火墙和入侵检测解决方案来保护其网络的安全,而防火墙和入侵检测解决方案发现不了 Web 的攻击行为。

1. 常见的 Web 应用安全漏洞

1) 已知弱点和错误配置

已知弱点包括 Web 应用使用的操作系统、第三方应用程序中的程序错误或者可以

被利用的漏洞。这个问题也涉及到错误配置,包含有不安全的默认设置或管理员没有进行安全配置的应用程序。一个很好的例子就是 Web 服务器被配置成可以让任何用户从任何目录路径通过,这样会导致泄露存储在 Web 服务器上的一些敏感信息,比如口令、源代码或客户信息等。

2) 隐藏字段

在许多应用中,隐藏的 HTML 格式字段被用来保存系统口令或商品价格。尽管其名称如此,但这些字段并不是很隐蔽的,任何在网页上执行"查看源代码"的人都能看见。许多 Web 应用允许恶意的用户修改 HTML 源文件中的这些字段,为他们提供了以极小成本或无需成本购买商品的机会。这些攻击行动之所以成功,是因为大多数应用没有对返回网页进行验证;相反,它们认为输入数据和输出数据是一样的。

3) 后门和调试漏洞

开发人员常常建立一些后门并依靠调试来排除应用程序的故障。在开发过程中这样做是无可非议的,遗憾的是,这些安全漏洞并没有被删除而是被保留在最终的应用程序中。一些常见的后门使攻击者不用口令就可以登录或者访问直接进行应用配置的特殊 URL。

4) 跨站点脚本编写

一般来说,跨站点编写脚本是将代码插入由另一个源发送的网页之中的过程。利用跨站点编写脚本的一种方式是通过 HTML 格式,将信息帖到公告牌上就是跨站点脚本编写的一个很好范例。恶意的用户会在公告牌上帖上包含有恶意的 JavaScript 代码的信息。当用户查看这个公告牌时,服务器除正常显示 HTML 网页内容以外,还自动运行附带的恶意代码,而且是在用户不知道的情况下悄悄地运行的。

5) 参数篡改

参数篡改包括操纵 URL 字符串,以检索用户用其他方式得不到的信息。访问 Web 应用的后端数据库是通过常常包含在 URL 中的 SQL 调用来进行的。恶意的用户可以操纵 SQL 代码,以便将来有可能检索一份包含所有用户、口令和信用卡号的清单或者储存在数据库中的任何其他数据。

6) 更改 Cookie

更改 Cookie 指的是修改存储在 Cookie 中的数据。网站常常将一些包括用户 ID、口令和账号等的 Cookie 存储到用户系统上。通过改变这些 Cookie 值,恶意的用户就可以访问不属于他们的账户。攻击者也可以窃取用户的 Cookie 并访问用户的账户,而不必输入 ID 和口令或进行其他验证。

7) 输入信息控制

输入信息检查是指通过控制由 CGI 脚本处理的、HTML 格式的输入信息来运行系统命令。

8) 缓冲区溢出

缓冲区溢出是恶意的用户向服务器发送大量数据以使系统瘫痪的典型攻击手段,该系统包括存储这些数据的预置缓冲区。如果所收到的数据量大于缓冲区,则部分数据就会溢出到堆栈中。如果这些数据是代码,系统随后就会执行溢出到堆栈上的任何代码。

Web 应用缓冲区溢出攻击的典型例子也涉及到 HTML 文件。如果 HTML 文件上的一个字段中的数据足够大,就能创造一个缓冲区溢出条件。

9) 直接访问浏览

直接访问浏览指直接访问应该需要验证的网页。没有正确配置的 Web 应用程序可以让恶意的用户直接访问包括有敏感信息的 URL。

2. 通过分析 Web 服务器记录查黑客攻击的踪迹

在这里,主要介绍如何分析 Web 服务器记录,在众多记录里查找黑客攻击的蛛丝马迹,并针对当今流行的两类 Web 服务器给出一些具体的措施。

现今的网络,安全越来越受到重视,在构建网络安全环境时,在技术手段及管理制度等方面都逐步加强了,设置防火墙,安装入侵检测系统等。但网络安全是个全方位的问题,忽略哪一点都会造成“木桶”效应,使得整个安全系统虚设。下面从分析 Web 服务器的 logging 记录来找出漏洞,防范攻击,从而加强 Web 服务器安全。

1) 默认的 Web 记录

对于 IIS,其默认记录存放在 c:\winnt\system32\logfiles\w3svc1 中,文件名就是当天的日期,记录格式是标准的 W3C 扩展记录格式,可以用各种记录分析工具解析,默认的格式包括时间、访问者 IP 地址、访问的方法、请求的资源和 HTTP 状态(用 3 位数字表示)等。对于 HTTP 状态,200～299 表明访问成功;300～399 表明需要客户端反应来满足请求;400～499 和 500～599 表明客户端和服务器出错,如 404 表示资源没找到,403 表示访问被禁止。

Apache 的默认记录存放在/usr/local/apache/logs 中,其中最有用的记录文件是 access_log,其格式包括客户端 IP、个人标识(一般为空)、用户名、访问方式、HTTP 状态和传输的字节数等。

2) 收集信息

可以模拟黑客攻击服务器的通常模式,先是收集信息,然后通过远程命令一步步实施入侵。

3) Web 站点镜像

黑客经常镜像一个站点来帮助攻击服务器,常用来镜像的工具有 Windows 下的 Teleport pro 和 UNIX 下的 Wget。

4) 漏洞扫描

随着攻击的发展,用户可以用一些 Web 漏洞检查的软件,如 Whisker,它可以检查已知晓的各种漏洞,如 CGI 程序导致的安全隐患等。

5) 远程攻击

可以针对 IIS 的 MDAC 攻击,来了解远程攻击在 log 里的记录情况。MDAC 漏洞使得攻击者可以在 Web 服务器端执行任何命令。

13.2.4 IP地址攻击

1. OOB **攻击**

OOB 是利用 NETBIOS 中一个 OOB(Out of Band,例外处理程序)的漏洞来进行攻击的,其原理是通过 TCP/IP 协议传递一个数据包到计算机某个开放的端口上(一般是 137、138 和 139),当计算机收到这个数据包之后就会瞬间死机或者出现蓝屏现象,不重新启动计算机就无法继续使用 TCP/IP 协议来访问网络。

2. DoS 攻击

这是针对 ICMP 协议进行的 DoS 攻击,一般来说,这种攻击是利用对方计算机上所安装协议的漏洞来连续发送大量的数据包,造成对方计算机的死机。

3. WinNuke 攻击

目前的 WinNuke 系列工具已经从最初的简单选择 IP 攻击某个端口发展到可以攻击一个 IP 区间范围的计算机,并且可以进行连续攻击,能够验证攻击的效果,还可以检测和选择端口,所以使用它可以造成某一个 IP 地址区间的计算机全部蓝屏死机。

4. SSPing 攻击

这是一个 IP 攻击工具,它的工作原理是向对方的计算机连续发出大型的 ICMP 数据包,被攻击的机器会试图将这些文件包合并处理,从而造成系统死机。

5. TearDrop 攻击

这种攻击方式利用在 TCP/IP 堆栈实现中信任 IP 碎片包的标题头所包含的信息来实现自己的攻击,由于 IP 分段中含有指示该分段所包含的是原包哪一段的信息,所以一些操作系统下的 TCP/IP 协议在收到含有重叠偏移的伪造分段时将崩溃。TeadDrop 最大的特点是除了能够对 Windows 2000/NT 进行攻击之外,Linux 也不能幸免。

13.2.5 电子邮件攻击

电子邮件是当今世界上使用最频繁的商务通信工具,据可靠统计显示,目前全球每天的电子邮件发送量已超过数百亿条,预计到 2008 年该数字还将增长一倍。

电子邮件的持续升温使之成为企图进行破坏的人所日益关注的目标。如今,黑客和病毒制造者在不断开发新的和有创造性的方法,以期突破网络的安全防范措施。

典型的互联网通信协议有 TCP 和 UDP 协议,其开放性常常引来黑客的攻击。而 IP 地址的脆弱性,也给黑客的伪造提供了方便,从而泄露远程服务器的资源信息。

很多电子邮件网关,对于过期的电子邮件地址,系统则回复发件人,告诉他们这些电子邮件地址无效。黑客则利用电子邮件系统这种内在“礼貌性”的信息来访问有效地址,并会将其添加到合法地址数据库中。

由于企业日益依赖于电子邮件系统，必须解决电子邮件传播的攻击和易受攻击的电子邮件系统所受的攻击。解决方法如下：

- 在电子邮件系统周围锁定电子邮件系统。电子邮件系统周边控制开始于电子邮件网关的部署。电子邮件网关应根据特定目标、要加固的操作系统和防止网关受到威胁的入侵检测功能一起构建。
- 确保外部系统访问的安全性。电子邮件安全网关必须负责处理来自所有外部系统的通信，并确保通过的信息流量是合法的。通过确保外部访问的安全，可以防止入侵者利用 Web 邮件等应用程序访问内部系统。
- 实时监视电子邮件流量。实时监视电子邮件流量对于防止黑客利用电子邮件访问内部系统是至关重要的。检测电子邮件中的攻击和漏洞攻击（如畸形 MIME）需要持续监视所有电子邮件。

在上述安全保障的基础上，电子邮件安全网关应简化管理员的工作，能够轻松集成、轻松配置。

13.2.6 拒绝服务攻击

1. 什么是拒绝服务攻击

拒绝服务攻击（DoS）是一种最悠久也是最常见的攻击形式。严格来说，拒绝服务攻击并不是某一种具体的攻击方式，而是攻击所表现出来的结果，最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或崩溃。具体的操作方法可以是多种多样的，可以是单一的手段，也可以是多种方式的组合利用，其结果都是一样的，即使合法用户无法正常访问系统。

通常拒绝服务攻击可分为两种类型：

第一种是使一个系统或网络瘫痪。如果攻击者发送一些非法的数据或数据包，就可以使系统死机或重新启动。本质上是攻击者进行了一次拒绝服务攻击，因为在受到拒绝服务攻击后没有人能够使用计算机网络资源。从攻击者的角度来看，攻击的刺激之处在于可以只发送少量的数据包就使一个网络系统瘫痪。在大多数情况下，系统重新上线需要管理员的干预，重新启动或关闭系统。所以这种攻击是最具破坏力的。

第二种攻击是向系统或网络发送大量信息，使系统或网络因为要回应和处理这些信息而不能响应其他服务。例如，如果一个网络系统在 1min 之内只能处理 5000 个数据包，攻击者却 1min 向他发送 10 000 个以上的数据包，这时，该网络系统的全部精力和时间都耗费在处理这些数据包上，当合法用户要连接系统时，用户将得不到访问权，因为系统资源已经不足。进行这种攻击时，攻击者必须连续地向系统发送数据包。当攻击者停止向该网络系统发送数据包时，攻击就会立即停止，系统也就恢复正常了。此攻击方法攻击者要耗费很多精力和时间，因为必须不断地发送数据。有时，这种攻击会使系统瘫痪，然而在大多数情况下，恢复系统只需要少量人为干预。

2. 拒绝服务攻击类型

1）Ping of Death

根据 TCP/IP 的规范，一个包的长度最大为 65 536B。尽管一个包的长度不能超过 65 536B，但是将一个包分成的多个片段的叠加却能做到发送超长包。当一个主机收到了长度大于 65 536B 的包时，就是受到了 Ping of Death 攻击，该攻击会造成主机的宕机。

2）TearDrop

IP 数据包在网络传递时，数据包可以分成更小的片段。攻击者可以通过发送两段或两段以上的数据包来实现 TearDrop 攻击。第一个包的偏移量为 0，长度为 N，第二个包的偏移量小于 N。为了合并这些数据段，TCP/IP 堆栈会分配超乎寻常的巨大资源，从而造成系统资源的不足而引起机器的重新启动。

3）Land

攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过 IP 欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而大大降低了系统性能。

4）Smurf

该攻击向一个子网的广播地址发一个带有特定请求（如 ICMP 回应请求）的包，并且将源地址伪装成想要攻击的主机地址。子网上所有主机都回应广播包请求而向被攻击主机发包，使该主机受到攻击。

5）SYN flood

该攻击以多个随机的源主机地址向目的主机发送 SYN 包，而在收到目的主机的 SYN ACK 后并不回应，这样，目的主机就为这些源主机建立了大量的连接队列，由于这些主机在没有收到 ACK 以前一直保持着这些连接队列，造成了资源的大量消耗而不能给正常请求提供服务。

6）CPU Hog

一种通过耗尽系统资源使运行 NT 的计算机瘫痪的拒绝服务攻击，利用 Windows NT 指定当前运行程序的方式所进行的攻击。

7）Win Nuke

是以拒绝目的主机服务为目标的网络层次的攻击。攻击者向受害主机的端口 139（即 NetBios）发送大量的数据。因为这些数据并不是目的主机所需要的，所以会导致目的主机的死机。

8）RPC Locator

攻击者通过 Telnet 连接到受害者机器的端口 135 上发送数据，导致 CPU 资源完全耗尽。这种攻击可以使受害计算机运行缓慢或者停止响应。无论哪种情况，要使计算机恢复正常运行速度必须重新启动。

3. 分布式拒绝服务攻击

分布式拒绝服务攻击（DDoS）是攻击者经常采用而且难以防范的攻击手段。DDoS

攻击是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的,当目标计算机处于 CPU 速度低、内存小或者网络带宽窄的时候,这种攻击的效果是很明显的。随着计算机与网络技术的发展,计算机的处理能力迅速增长,内存大大增加,同时也出现了千兆级别甚至万兆级别的网络,这使得单一的 DoS 攻击困难程度加大了,目标对恶意攻击包的"消化能力"加强了不少,例如,设攻击软件 1s 可以发送 1000 个攻击包,而目标主机与网络带宽 1s 可以处理 10 000 个攻击包,这样一来攻击就不会产生什么效果,所以分布式的拒绝服务攻击手段(DDoS)就应运而生了。如果用一台攻击机来攻击不起作用的话,攻击者就使用 10 台、100 台甚至成千上万台攻击机同时向目标主机发起攻击。

DDoS 就是利用更多的傀儡机来发起进攻,以比从前更大的规模来进攻受害者。

高速广泛连接的网络也为 DDoS 攻击创造了极为有利的条件。在低速网络时代,黑客占领攻击用的傀儡机时,总是会优先考虑离目标网络距离近的计算机,因为经过路由器的跳数少,效果好。而现在电信骨干结点之间的连接都是以 GB 为级别的,大城市之间更可以达到 2.5G 以上的连接,这使得攻击可以从更远的地方或者其他城市发起,攻击者的傀儡机位置可以分布在更大的范围,选择起来更灵活了。

一个完善的 DDoS 攻击体系分成四大部分:

- 攻击者所在机;
- 控制机(用来控制傀儡机);
- 傀儡机;
- 受害者。

4. 拒绝服务攻击工具

1) Targa

可以进行 8 种不同的拒绝服务攻击,设计者是 Mixter,可以在 http://packerstorm.security.com 和 www.rootshell.com 网站下载。Mixter 把独立的 DoS 攻击代码放在一起,做出一个易用的程序。攻击者可以选择进行单个的攻击或尝试所有的攻击,直到成功为止。

2) TFN2K

TFN2K 可以看作是 Traga 增强版本程序。TFN2K 运行的 DoS 攻击与 Traga 相同,并增加了 5 种攻击。另外,它是一个 DDoS 工具,这意味着它可以运行分布模式,即利用 TFN2K 可以联合 Internet 上的多台计算机同时攻击某一台计算机或某一个网站。

3) Trinoo

Trinoo 是发布最早的主流工具,因而在功能上比 TFN2K 稍弱。Trinoo 使用 TCP 和 UDP 连接,如果用扫描程序检测端口,该攻击很容易被检测到。

4) Stacheldraht

Stacheldraht 是另一个 DDoS 攻击工具,它结合了 TFN2K 与 Trinoo 的特点,并添加了一些补充特征,比如加密组件之间的通信和自动更新守护进程。

13.3 黑客防范技术

13.3.1 入侵检测技术及端口扫描技术

1. 入侵检测技术

入侵检测(intrusion detection)的定义为：识别针对计算机或网络资源的恶意企图和行为，并对此作出反应的过程。入侵检测系统(IDS)则是完成如上功能的独立系统。IDS能够检测未授权对象(人或程序)针对系统的入侵企图或行为(Intrusion)，同时监控授权对象对系统资源的非法操作(misuse)。入侵检测系统有如下功能：

- 从系统的不同环节收集信息。
- 分析该信息，试图寻找入侵活动的特征。
- 自动对检测到的行为做出响应。
- 纪录并报告检测过程结果。

2. 端口扫描技术

前面介绍过，“端口扫描”通常指将同一组信息发送给目标计算机的所有需要扫描的端口，然后根据返回端口状态来分析目标计算机的端口是否打开、是否可用。

入侵检测技术与端口扫描技术详见本书第10章。

13.3.2 清除主机中的Cookie

1. 什么是Cookie

Cookie(网络小甜饼)为Web应用程序保存用户相关信息提供了一种有用的方法。例如，当用户访问某个站点时，可以利用Cookie保存用户首选项或其他信息，这样，当用户下次再访问这个站点时，应用程序就可以检索Cookie以前保存的信息，以加快查找速度。

Cookie是一小段文本信息，伴随着用户请求和页面在Web服务器和浏览器之间传递。用户每次访问站点时，Web应用程序都可以读取Cookie包含的信息。

假设在用户请求访问网站www.contoso.com上的某个页面时，应用程序发送给该用户的不仅仅是一个页面，还有一个包含日期和时间的Cookie。用户的浏览器在获得页面的同时还得到了这个Cookie，并且将它保存在用户硬盘上的某个文件夹中。

以后，如果该用户再次访问该站点上的页面，即当该用户输入www.contoso.com时，浏览器就会在本地硬盘上查找与该URL相关联的Cookie。如果该Cookie存在，浏览器就将它与页面请求一起发送到此站点，应用程序就能确定该用户上一次访问站点的日期和时间。可以根据这些信息向用户发送一条消息，也可以检查过期时间或执行其他有用的功能。

Cookie 是与 Web 站点有关联的，所以无论用户请求浏览站点中的哪个页面，浏览器和服务器都将交换 www.contoso.com 的 Cookie 信息。用户访问其他站点时，每个站点都可能会向用户浏览器发送一个 Cookie，而浏览器会将这些 Cookie 分别保存。

用户可用 Cookie 文件保存上网痕迹，以方便下次再次浏览相关网站时能够快速定位，以提高网络访问速度和效率。另一方面，黑客在访问用户的网络或网站后，也会利用 Cookie 文件在用户的主机上保存痕迹，以方便下一次攻击，因此，Cookie 文件对用户的计算机、网络和网站是有一定的威胁和风险的，因此，有必要经常删除主机中的 Cookie 文件，以确保网络的安全。

2. Cookie 的删除

在 IE 浏览器中，选择"工具"|"Internet 选项"，出现如图 13-1 所示的窗口。



图 13-1　Internet 选项

在图 13-1 所示的窗口中，单击"删除 Cookies"按钮，即将主机中所有保留的 Cookie 全部清除。

13.3.3　木马的清除与防范技术

1. 何谓木马

在古希腊进攻特洛伊的一次战争中，特洛伊城久攻不下，谋士给指挥官出了一个绝妙的计谋。于是，在一次猛烈的攻城战斗结束后的黄昏，希腊人装败全线撤退，并丢弃了大量物品和内藏士兵的木马在特洛伊城外，特洛伊人在打扫战场时，将所有的木马当作战利器悉数拖入城中，当晚，藏在木马中的希腊士兵与城外的攻城大军里应外合，一举攻破了特洛伊城，特洛伊木马的名称也就由此而来。在计算机里，木马指的是一种隐蔽性极强、破坏性极大的病毒软件。

木马实质上是一种网络病毒，但它通常作为黑客的主要攻击工具，所以作者将木马的清除与防范技术放在本章中进行介绍而不放在第12章。

木马主要目标是窃取计算机和网络上的数据，当然也会破坏计算机文件，当用户的计算机被木马攻击后，木马一旦激活，则后缀为dll、in、exe的文件就是木马攻击的对象，将会给用户的计算机和网络以致命的攻击。

木马程序不同于一般的病毒程序，通常并不像病毒程序那样感染文件。木马一般是以寻找后门、窃取密码和重要文件为主，还可以对计算机进行跟踪监视、控制、查看和修改资料等操作，具有很强的隐蔽性、突发性和攻击性。由于木马具有很强的隐蔽性，用户往往是在自己的密码被盗、机密文件丢失的情况下才知道自己中了木马。在这里将介绍如何检测自己的计算机是否中了木马，如何对木马进行清除和防范。

2. 黑客是如何种植木马的

现在网络上流行的木马基本上采用的都是C/S结构(客户端/服务端)。若要使用木马控制对方的计算机，首先需要在对方的计算机中种植并运行服务端程序，然后再运行本地计算机中的客户端程序对对方计算机进行连接进而控制对方计算机。

为了避免不熟悉木马的用户误运行服务端程序，现在流行的木马都没有提供单独的服务端程序，而是通过用户自己设置来生成服务端程序，“黑洞2004”就是这样一种木马。首先运行“黑洞2004”，单击“功能”|“生成服务端”命令，弹出“服务端配置”界面。之后，先单击旁边的“查看”按钮，在打开的窗口中设置新的域名，输入用户事先申请空间的域名和密码，单击“域名注册”，在下面的窗口中会反映出注册的情况。域名注册成功以后，返回“服务端配置”界面，填入刚刚申请的域名以及“上线显示名称”、“注册表启动名称”等项目。为了迷惑他人，可以单击“更改服务端图标”按钮为服务端选择一个图标。所有的设置都完成后，单击“生成EXE型服务端”就生成了一个服务端程序。在生成服务端程序的同时，软件会自动使用UPX为服务端进行压缩，对服务端起到隐藏保护的作用。

服务端程序生成以后，下一步要做的是将服务端程序植入别人的计算机，常见的方法有，通过系统或者软件的漏洞入侵别人的计算机并把木马的服务端程序植入其计算机中；或者通过E-mail夹带，把服务端作为附件寄给对方；或者把服务端进行伪装后放到自己的共享文件夹，通过P2P软件让网友在毫无防范中下载并运行服务端程序。

在这里介绍一种较为简单的E-mail夹带，以经常会看到的Flash动画为例，建立一个文件夹命名为“好看的动画”，在该文件夹里边再建立文件夹“动画.files”，将木马服务端软件放到该文件夹中并假设文件名称为abc.exe，再在该文件夹内建立flash文件，在flash文件的第1帧输入文字“您的播放插件不全，单击下边的按钮，再单击‘打开’按钮安装插件”，新建一个按钮组件，将其拖到舞台中，打开动作面板，在里边输入“on (press){getURL("动画.files/abc.exe");}”，表示当单击该按钮时执行abc文件。在文件夹“好看的动画”中新建一个网页文件，命名为“动画.html”，将刚才制作的动画放到该网页中。平常下载的网站通常就是一个.html文件和一个结尾为.files的文件夹，这样构造的原因也是用来迷惑打开者，毕竟没有几个人会去翻.files文件夹。现在就可以撰写一封新邮件了，将文件夹“好看的动画”压缩成一个文件，放到邮件的附件中，再编写一个诱人的主

题。只要对方深信不疑地运行它，并重新启动系统，服务端就种植成功了。

3. 使用木马

成功地给别人植入木马服务端后，就需要耐心等待服务端上线。由于“黑洞 2004”采用了反连接技术，所以服务端上线后会自动和客户端进行连接，这时，就可以用客户端对服务端进行远程控制。在“黑洞 2004”下面的列表中，随便选择一台已经上线的计算机，然后通过界面上的命令按钮就可以对这台计算机进行控制。下面就介绍这些命令按钮的意义和功能。

- 文件管理。服务端上线以后，可以通过“文件管理”命令对服务端计算机中的文件进行下载、新建、重命名和删除等操作。可以通过鼠标直接把文件或文件夹拖放到目标文件夹，并且支持断点传输。
- 进程管理。查看、刷新、关闭对方的进程，如果发现有杀毒软件或者防火墙，就可以关闭相应的进程，达到保护服务器端程序的目的。
- 窗口管理。管理服务端计算机的程序窗口，可以对对方窗口中的程序进行最大化、最小化和正常关闭等操作，这样就比进程管理更灵活。也可以搞很多恶作剧，比如让对方的某个窗口不停地最大化和最小化。
- 视频监控和语音监听。如果远程服务端计算机安装有 USB 摄像头，可以通过它来获取图像，并可直接保存为 Media Play 和可以直接播放的 Mpeg 文件；若对方有麦克风，还可以听到他们的谈话。

除了上面介绍的这些功能以外，还包括键盘记录、重启关机、远程卸载和抓屏查看密码等功能，操作都非常简单。

4. 木马的隐藏技术

随着杀毒软件病毒库的升级，木马很快就会被杀毒软件查杀，为了使木马服务端避开杀毒软件的查杀，长时间地隐藏在别人的计算机中，黑客通常用下列方法来隐藏木马：

1）木马的自身保护

就像前面提到的，“黑洞 2004”在生成服务端的时候，可以更换图标，并使用软件 UPX 对服务端自动进行压缩隐藏。

2）捆绑服务端

通过使用文件捆绑器把木马服务端和正常的文件捆绑在一起，达到欺骗对方的目的。文件捆绑器有广外文件捆绑器 2002、万能文件捆绑器、exeBinder 和 Exe Bundle 等。

3）制作自己的服务端

上面提到的这些方法虽然能一时瞒过杀毒软件，但最终还是不能逃脱杀毒软件的查杀，所以若能对现有的木马进行伪装，让杀毒软件无法辨别，则是个治本的方法。可以通过使用压缩 EXE 和 DLL 文件的压缩软件对服务端进行加壳保护。例如 Step1 中的 UPX 就是这样一款压缩软件，但默认该软件是按照自身的设置对服务端压缩的，因此得出的结果都相同，很难长时间躲过杀毒软件的检测；而自己对服务端进行压缩，就可以选择不同的选项，压缩出与众不同的服务端来，使杀毒软件很难判断。下面以“冰河”木马

为例，简要介绍木马脱壳(解压)、加壳(压缩)的过程。

如果用杀毒软件对冰河进行查杀，一定会发现2个病毒，一个是冰河的客户端，另一个是服务端。还可以使用软件PEiD查看软件的服务端是否已经被作者加壳。

现在，需要对软件进行脱壳，也就是一种解压的过程。这里使用UPXUnpack，选择需要的文件后，单击"解压缩"就开始执行脱壳。

脱壳完成后，需要为服务端加一个新壳，加壳的软件很多，比如ASPack、ASProtect、UPXShell和Petite等。这里以ASPack为例，单击"打开"按钮，选择刚刚脱壳的服务端程序，选择完成后ASPack会自动为服务端进行加壳。再次用杀毒软件对这个服务端进行查杀，发现其已经不能识别判断了。如果用户的杀毒软件依旧可以查杀，就可以使用多个软件对服务端进行多次加壳。现在网络中流行的很多版本的"冰河"，就是网友通过对服务端进行修改并重新加壳后制作出来的。

5. 木马的检测技术

1) 查看开放端口

当前最为常见的木马通常是基于TCP/UDP协议进行client端与server端之间的通信的，这样就可以通过在本机上开放的端口，查看是否有可疑的程序打开了某个可疑的端口。例如冰河使用的监听端口是7626，Back Orifice 2000使用的监听端口是54320等。假如查看到有可疑的程序在利用可疑端口进行连接，则很有可能就是中了木马。查看端口的方法有下面几种：

(1) 使用Windows本身自带的netstat命令检测。

```
C:\> netstat -an
```

(2) 使用Windows 2000下的命令行工具fport。

```
c:\\software> Fport.exe
```

(3) 使用图形化界面工具Active Ports。

这个工具可以监视到计算机所有打开的TCP/IP/UDP端口，还可以显示所有端口所对应的程序所在的路径，本地IP和远端IP(试图连接用户的计算机IP)是否正在活动。这个工具适用于Windows NT/2000/XP平台。

2) 查看win.ini和system.ini系统配置文件

查看win.ini和system.ini文件是否有被修改的地方。例如有的木马通过修改win.ini文件中windows节 的load=file.exe ,run=file.exe语句进行自动加载。此外可以修改system.ini中的boot节，实现木马加载。例如"妖之吻"病毒，将Shell=Explorer.exe(Windows系统的图形界面命令解释器)修改成Shell=yzw.exe，在计算机每次启动后就自动运行程序yzw.exe。修改的方法是将shell=yzw.exe还原为shell=explorer.exe。

3) 查看启动程序

如果木马自动加载的文件是直接通过在Windows菜单上自定义添加的，一般都会放在主菜单的"开始|程序|启动"处，在Windows资源管理器里的位置是"C:\windows\start menu\programs\启动"处。通过这种方式使文件自动加载时，一般都会将其存放在

注册表中下述 4 个位置上：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
```

检查是否有可疑的启动程序，便很容易查到是否中了木马。

在 Windows 系统下，还可以直接运行 Msconfig 命令查看启动程序和 system. ini、win. ini、autoexec. bat 等文件。

4）查看系统进程

木马即使再狡猾，它也是一个应用程序，需要进程来执行。可以通过查看系统进程来推断木马是否存在。

在 Windows NT/XP 系统下，按 Ctrl+Alt+Del 组合键，进入任务管理器，就可看到系统正在运行的全部进程。在 Windows 下，可以通过 Preview 和 winproc 工具来查看进程。查看进程，要求用户对系统非常熟悉，对每个系统运行的进程要知道它是做什么用的，这样，若有木马进程正在运行，就很容易看出来哪个是木马程序的活动进程了。

5）查看注册表

木马一旦被加载，一般都会对注册表进行修改。一般来说，木马在注册表中实现加载文件一般是在以下位置：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
```

6）使用检测软件

上面介绍的是手工检测木马的方法，此外，还可以通过各种杀毒软件、防火墙软件和各种木马查杀工具等检测木马。杀毒软件主要有 KV3000、Kill3000 和瑞星等，防火墙软件主要有国外的 Lockdown，国内的天网、金山网镖等，各种木马查杀工具主要有 The Cleaner、木马克星和木马终结者等。

6. 普通木马的清除技术

检测到计算机中了木马后，就要根据木马的特征来进行清除。查看是否有可疑的启动程序、可疑的进程存在，是否修改了 win. ini、system. ini 系统配置文件和注册表。如果存在可疑的程序和进程，就按照特定的方法进行清除。

1）删除可疑的启动程序

查看系统启动程序和注册表是否存在可疑的程序后，判断是否中了木马，如果存在木马，则除了要查出木马文件并删除外，还要将木马自动启动程序删除。例如 Hack.

Rbot 病毒、后门就会复制自身到一些固定的 Windows 自启动项中：

```
WINDOWS\All Users\Start Menu\Programs\StartUp
WINNT\Profiles\All Users\Start Menu\Programs\Startup
WINDOWS\Start Menu\Programs\Startup
Documents and Settings\All Users\Start Menu\Programs\Startup
```

查看一下这些目录，如果有可疑的启动程序，则将之删除。

2）恢复 win. ini 和 system. ini 系统配置文件的原始配置

许多病毒会将 win. ini 和 system. ini 系统配置文件修改，使之能在系统启动时加载和运行木马程序。例如计算机中了“妖之吻”病毒后，病毒会将 system. ini 中的 boot 节的“Shell＝Explorer. exe”字段修改成“Shell＝yzw. exe”，清除木马的方法是把 system. ini 给恢复原始配置，即“Shell＝yzw. exe”修改回“Shell＝Explorer. exe”，再删除掉病毒文件即可。

TROJ_BADTRANS. A 病毒，也会更改 win. ini 以便在下一次重新开机时执行木马程序。主要是将 win. ini 中的 windows 节的“Run＝”字段修改成“Run＝ C：％WINDIR％INETD. EXE”字段。执行清除的步骤如下：

- 打开 win. ini 文本文件，将字段“RUN＝C：％WINDIR％INETD. EXE”中等号后面的字符删除，仅保留“RUN＝”。
- 将被 TROJ_BADTRANS. A 病毒感染的文件删除。

3）停止可疑的系统进程

木马程序在运行时都会在系统进程中留下痕迹。通过查看系统进程可以发现运行的木马程序，在对木马进行清除时，当然首先要停掉木马程序的系统进程。例如 Hack. Rbot 病毒、后门除了将自身复制到一些固定的 Windows 自启动项中外，还在进程中运行 wuamgrd. exe 程序，修改了注册表，以便病毒可随机自启动。若看到有木马程序在进程中运行，则需要马上杀掉该进程，并进行下一步操作，修改注册表和清除木马文件。

4）修改注册表

查看注册表，将注册表中木马修改的部分还原。例如上面所提到的 Hack. Rbot 病毒、后门，向注册表的以下地方：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

添加键值“Microsoft Update”＝“wuamgrd. exe”，以便病毒可随机自启动。这就需要用户进入注册表，将这个键值删除。

下面介绍如何清除 Hack. Rbot 病毒：

- 停止 wuamgrd. exe 进程，这是一个木马程序。
- 将 Hack. Rbot 复制到 Windows 启动项中的启动文件删除。
- 将 Hack. Rbot 添加到注册表中的键值“Microsoft Update”＝“wuamgrd. exe”

删除。

- 手工或用专杀工具删除被 Hack. Rbot 病毒感染的文件,并全面检查系统。

5) 使用杀毒软件和木马查杀工具查杀木马

常用的杀毒软件包括 KV3000、瑞星和诺顿等,这些软件对木马的查杀是比较有效的,但是要注意时刻更新病毒库,而且对于一些木马查杀不彻底,在系统重新启动后还会自动加载。此外,还可以使用 The Cleaner、木马克星和木马终结者等各种木马专杀工具对木马进行查杀。这里推荐一款工具 Anti-Trojan Shield,这是一款享誉欧洲的专业木马侦测、拦截及清除软件,可以在 http://www. atshield. com 网站下载。

7. 几种特殊木马的清除技术

由于木马的种类很多,对不同的木马,其清除技术也不尽相同。下面,介绍几种常见特殊木马的清除技术。

1) BO 木马

BO(Back Orifice)是一种没有任何权限限制的 FTP 服务器程序,黑客先使用各种方法诱惑他人使用 BO 的服务器端程序,一旦得逞便可通过 BO 客户端程序经由 TCP/IP 网络进入并控制远程的 Windows。其工作原理是,Boserve. exe 在对方的计算机中运行后,自动在 Windows 里注册并隐藏起来,在对方上网后通过 Boconfig. exe(安装设置的程序)和 Boclient. exe(文本方式的控制程序)或 Bogui. exe(图形界面控制程序)来控制对方。网上更有一些害人虫将木马程序和其他应用程序结合起来发送给对方,只要对方运行了 BO 程序,木马就会驻留到 Windows 系统中,BO 本质上属于客户机/服务器应用程序。它通过一个极其简单的图形用户界面和控制面板,可以对感染了 BO(即运行了 BO 服务器)的计算机操作 Windows 本身具备的所有功能。BO 没有利用系统和软件的任何漏洞或 Bug,也没有利用任何微软未公开的内部 API,而完全是利用 Windows 系统的设计缺陷。甚至连普通的局域网防火墙和代理服务器也难以抵挡。BO 服务器可通过网上下载、电子邮件、盗版光盘和人为投放等途径传播,并且可极其隐蔽地粘贴在其他应用程序中。一旦激活,就可以自动安装,创建 Windll. dll,然后删除自安装程序,埋名隐姓,潜伏在计算机中。入侵者就可通过 BO 客户机程序,方便地搜索到世界上任何一台被 BO 感染并上网的计算机 IP 地址。通过 IP 地址就可对其轻易实现网络和系统控制功能。可获取包括网址口令、拨号上网口令、用户口令、磁盘、CPU 和软件版本等详细的系统信息;可删除、复制、检查、查看文件;可运行计算机机内任何一个程序;可捕捉屏幕信息;可上传各种文件;可以查阅、创建、删除和修改系统注册表;可以使计算机重新启动或锁死机器。而所有这些功能的实现,只需在菜单中作一选择,轻按一键,就可轻松完成。

Back Orifice 2000 的防范技术:

(1) 对于 95 和 98 的用户,检查 C:\windows\system 目录下是否有 UMGR32~1. exe 文件,如果存在则运行 Regedit,将 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices 中的 UMGT32. exe 清除,重启计算机,然后用 Delete 命令删除硬盘上的 UMGT32. exe 文件。

(2) 对于 NT 的用户,检查 C:\winnt\system32 目录下是否有 UMGR32~1. exe 这个

文件，如果有的话先将任务管理器中对应的进程 Kill 掉，再运行 Regedit 并将路径指向 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Remote Administration Service，然后删除它，最好重启一次计算机。

BO 的清除步骤：

(1) 运行 Regedit.exe，打开注册表。

(2) 选择目录至 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices。

(3) 查找并删除键值为“.exe”的键值。

(4) 关闭 Regedit，重新启动计算机。

(5) 将 C:\Windows\System 目录下的“.exe”删除，然后，再删除 Windll.dll 文件。

(6) 再次重新启动计算机。

2) 冰河木马

冰河木马是用 C++ Builder 写的，为了便于理解，将用 VB 来说明，其中涉及到一些 WinSock 编程和 Windows API 的知识，如果对此不是很了解的话，请查阅相关的资料。

清除过程如下：

(1) 运行 Regedit.exe，打开注册表。

(2) 选择目录至 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\RUN。

(3) 查找并删除“C:\Windows\System”文件夹下的“kernel32.exe”和“Sysexplr.exe”两个键值。

(4) 关闭 Regedit，重新启动计算机。

(5) 删除“C:\Windows\System\kernel32.exe”和“C:\Windows\System\Sysexplr.exe”两个文件。

(6) 再次重新启动计算机。

3) netspy 木马的清除

(1) 运行 Regedit.exe，打开注册表。

(2) 选择目录至 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RUN。

(3) 查找并删除 SysProtect=“C:\Windows\System\System.exe”或 Netspy=“Netspy.exe”键值。

(4) 关闭 Regedit，重新启动计算机。

(5) 删除“C:\Windows\System”目录下的“System.exe”和“Netspy.exe”两个文件。

(6) 再次重新启动计算机。

4) SubSeven 木马的清除

(1) 运行 Regedit.exe，打开注册表。

(2) 选择目录至 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RUN。

(3) 查找并删除 SystemTraylcon="C:\Windows\SysTraylcon.exe"键值。

(4) 关闭 Regedit,重新启动计算机。

(5) 删除"C:\Windows"目录下的"SysTraylcon.exe"文件。

(6) 再次重新启动计算机。

8. 木马的防范技术

随着网络的普及,硬件和软件的高速发展,网络安全显得日益重要。对于网络中比较流行的木马程序,传播时间比较快,影响比较严重,因此对于木马的防范就更不能疏忽。在检测清除木马的同时,还要注意对木马的预防,做到防患于未然。

1) 不要随意打开来历不明的邮件

现在许多木马都是通过邮件来传播的,当收到来历不明的邮件时,请不要打开,应尽快删除。并加强邮件监控系统,拒收垃圾邮件。

2) 不要随意下载来历不明的软件

最好是在一些知名的网站下载软件,不要下载和运行那些来历不明的软件。在安装软件的同时最好用杀毒软件查看有没有病毒,之后再进行安装。

3) 及时修补漏洞和关闭可疑的端口

一般木马都是通过漏洞在系统上打开端口留下后门,以便上传木马文件和执行代码,在把漏洞修补上的同时,需要对端口进行检查,把可疑的端口关闭。

4) 尽量少用共享文件夹

如果必须使用共享文件夹,则最好设置账号和密码保护。注意千万不要将系统目录设置成共享,最好将系统下默认共享的目录关闭。Windows 系统默认情况下将目录设置成共享状态,是非常危险的。

5) 运行实时监控程序

在上网时最好运行反木马实时监控程序和个人防火墙,并定时对系统进行病毒检查。

6) 经常升级系统和更新病毒库

经常关注厂商网站的安全公告,这些网站通常都会及时地将漏洞、木马和更新公布出来,并在第一时间发布补丁和新的病毒库等。

13.4 应用实例

13.4.1 个人计算机防"黑"技术

当用户在网络上冲浪、聊天或发电子邮件时,必须要有共同的协议,这个协议就是 TCP/IP 协议。如果把互联网比作公路网,计算机就是路边的房屋,房屋要有门才可以进出,TCP/IP 协议规定,计算机可以有 256×256 扇门,即从 0 到 65 535 号"门",TCP/IP 协议把它叫做"端口"。当用户发电子邮件的时候,E-mail 软件把信件送到了邮件服务器的 25 号端口,当收信的时候,E-mail 软件是从邮件服务器的 110 号端口这扇门进去取信的。新安装好的个人计算机打开的端口号是 139 端口,上网的时候,就是通过这个端口

与外界联系的。黑客正是通过端口进入用户的计算机和网站的。

1. 通过端口进入用户的计算机

黑客是怎么样进入用户计算机的呢？当然也是基于 TCP/IP 协议，通过某个端口进入用户个人计算机的。如果用户的计算机设置了共享目录，那么黑客就可以通过 139 端口进入用户的计算机，注意，Windows 系统有个缺陷，无论共享目录设置了多长的密码，黑客都能进入用户的计算机，所以，最好不要设置共享目录，这样就能防止别人浏览自己计算机上的资料。除了 139 端口以外，如果没有别的端口是开放的，黑客就不能入侵用户的个人计算机。那么黑客怎么样才会进到用户的计算机中的呢？答案是通过特洛伊木马进入。如果用户不小心运行了特洛伊木马，计算机上的某个端口就会开放，黑客就通过这个端口进入。举个例子，有一种典型的木马软件，叫做 netspy. exe。如果用户不小心运行了 netspy. exe，那么它就会告诉 Windows，以后每次开计算机的时候都要运行它，然后，netspy. exe 又在用户的计算机上开了一扇“门”，“门”的编号是 7306 端口，如果黑客知道用户的 7306 端口是开放的话，就可以用软件偷偷进入到用户的计算机中。特洛伊木马本身就是为了入侵个人计算机而制作的，它藏在计算机中，在工作的时候都是很隐蔽的，它的运行和黑客的入侵，不会在计算机的屏幕上显示出任何痕迹。Windows 本身没有监视网络的软件，所以不借助软件，是不知道特洛伊木马的存在和黑客的入侵的。

2. 如何发现自己计算机中的木马

在这里，仍以 netspy. exe 为例，假若知道 netspy. exe 打开了计算机的 7306 端口，要想知道自己的计算机是不是中了 netspy. exe，只要敲敲 7306 这扇“门”就可以了。先打开 C：\WINDOWS\WINIPCFG. EXE 程序，首先找到自己的 IP 地址（比如用户的 IP 地址是 210. 40. 100. 10），然后打开浏览器，在浏览器的地址栏中输入 http：//210. 40. 100. 10：7306/，如果浏览器告诉用户连接不上，说明用户的计算机的 7306 端口没有开放；如果浏览器能连接上，并且在浏览器中跳出一排英文说明及 netspy. exe 的版本，那么说明计算机中了 netspy. exe 木马。这是最简单最直接的办法，但是需要知道各种木马所开放的端口。下列端口是木马常用的开放端口：

7306、7307、7308、12345、12345、12346、31337、6680、8111、9910。

3. 进一步查找木马

有人曾经做过一个试验，假设被攻击用户已知 netspy. exe 开放的是 7306 端口，于是用工具把它的端口修改，经过修改的木马开放的是 7777 端口，现在再用旧的办法是找不到 netspy. exe 木马的。于是可以用扫描计算机的办法看看计算机有多少端口开放着，并且再分析这些开放的端口。

网络的端口号是 0～65 535，其中 139 端口在正常情况下应该是开放的，用户可以关闭正在运行的 139 端口，然后再用端口扫描软件对 0～65 535 端口扫描，如果除了 139 端口以外还有其他的端口开放，那么很可能是木马造成的。

排除了 139 端口以外的端口，可以进一步进行分析，用浏览器进入这个端口看看，它

会做出什么样的反应，就可以根据情况再判断了。

4. 在硬盘上删除木马

最简单的办法当然是用杀毒软件删除木马了，Netvrv病毒防护墙可以帮助用户删除netspy.exe和bo.exe木马，但是不能删除netbus木马。

下面就netbus木马为例介绍删除过程。

netbus木马的客户端有两种，一种以Mring.exe为代表(472 576B)，另一种以SysEdit.exe为代表(494 592B)，netbus木马开放的都是12345端口。

Mring.exe一旦被运行以后，Windows每次启动时都会自动运行Mring.exe，因为Windows将它放在了注册表中，用户可以打开注册表C:\WINDOWS\REGEDIT.EXE，然后进入HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run找到Mring.exe，然后删除这个键值，再到Windows中找到并删除Mring.exe文件。注意，Mring.exe可能会被黑客改变名字，字节长度也会被改变，但是在注册表中的位置不会改变，可以到注册表的这个位置去查找。

另外，可以找包含有netbus字符的可执行文件，再看字节的长度，Windows和其他的一些应用软件没有包含netbus字符的，被找到的文件多半就是Mring.exe的变种。

要知道自己的计算机中有没有木马，只要看看有没有可疑端口被开放，用代理猎手、Tcpview.exe都可以查找。要查找木马，一是可以到注册表的指定位置去找；二是可以查找包含相应的可执行程序，比如，被开放的端口是7306，就找包含netspy的可执行程序；三是检视内存，看有没有相关的程序在内存中。

5. 悄悄等待黑客的来临

在这里，介绍两款实用软件，使用这两款软件，可以捕获木马对本机和网站的攻击。

NukeNabber是一款端口监视器软件，用NukeNabber监视7306端口，如果有人接触这个端口，就马上报警。在别人看来，你的计算机的7306端口是开放的，但是7306不是由netspy控制，当NukeNabber发现有人接触7306端口或者试图进入自己的7306端口，会马上报警，用户可以在NukeNabber上面看到黑客做了些什么，黑客的IP地址是哪里，然后，就可以反过来攻击黑客了。当用NukeNabber监视139端口的时候，就可以知道谁在用IP炸弹炸自己。如果NukeNabber告诉用户不能监视7306端口，说明这个端口已经被占用了，也说明用户的计算机中已经存在了netspy木马。

第二个软件就是Tcpview.exe，这个软件是线程监视器，可以用它来查看有多少端口是开放的，有哪些用户在和自己通信，对方的IP地址和端口分别是什么。

13.4.2 “蜜罐”诱骗技术

1. 什么叫蜜罐

蜜罐，或称Honeypot，就是使用一台不作任何安全防范措施而且连接网络的计算

机，但是与一般计算机不同的是，它内部运行着多种多样的数据记录程序和特殊用途的"自我暴露程序"，在"蜜罐"中加上了很多"蜂蜜"，用以诱惑贪嘴的"黑熊"上钩。从入侵者的角度来看，入侵到蜜罐会使他们的心情大起大落，从一开始偷着乐骂管理员傻帽到最后明白自己被傻帽当成猴子耍的过程。

2. 为什么要使用蜜罐

前面说过了，"蜜罐"是一台"故意"存在多种漏洞的计算机，而且管理员清楚它身上有多少个漏洞，这就像狙击手为了试探敌方狙击手的实力而用枪支撑起的钢盔，蜜罐会记录入侵者的一举一动，为管理员能更好地分析入侵者都喜欢往哪个洞里钻，以便加强防御。

另一方面是因为防火墙的局限性和脆弱性，因为防火墙必须建立在基于已知危险的规则体系上进行防御，如果入侵者发动新形式的攻击，防火墙没有相对应的规则去处理，这时的防火墙就形同虚设，防火墙保护的系统也会遭到破坏，因此技术员需要蜜罐来记录入侵者的行动和入侵数据，必要时给防火墙添加新规则或者手工防御。

3. 蜜罐技术

可能会有人问，既然使用蜜罐能有那么多好处，那么大家都可在家里做个蜜罐，岂不是能最大程度防范黑客？蜜罐虽然在一定程度上能帮管理员解决分析问题，但它并不是防火墙，相反的，它也是一个危险的入侵系统。蜜罐会被狡猾的入侵者反利用来攻击别人的例子也屡见不鲜，只要管理员在某个设置上出现错误，蜜罐就成了打狗的肉包子。虽然蜜罐要做好随时牺牲的准备，如果到最后都没能记录到入侵数据，那么这台蜜罐纯粹就是等着挨宰的肉鸡了。蜜罐的复杂性就在此，它自身需要提供让入侵者乐意停留的漏洞，又要确保后台记录能正常而且隐蔽地运行，这些都需要高超的专业技术。

首先要弄清楚一台蜜罐和一台没有任何防范措施的计算机的区别，虽然这两者都有可能被入侵破坏，但是本质却完全不同，蜜罐是网络管理员经过周密布置而设下的"黑匣子"，看似漏洞百出却尽在掌握之中，它收集的入侵数据十分有用；一般的计算机根本就是送给入侵者的礼物，即使被入侵也不一定查得到痕迹。因此，蜜罐的定义是，"蜜罐是一个安全资源，它的价值在于被探测、攻击和损害的同时，记录下入侵的一切行为。"

设计蜜罐的初衷就是让黑客入侵，借此收集证据，同时隐藏真实的服务器地址，因此要求一台合格的蜜罐必须具有的发现攻击、产生警告、强大的记录能力、欺骗、协助调查的功能。另外一个功能由管理员去完成，那就是在必要时候根据蜜罐收集的证据来起诉入侵者。

4. 蜜罐的类型

1）实系统蜜罐

实系统蜜罐是最真实的蜜罐，它运行着真实的系统，并且带着真实可入侵的漏洞，属于最危险的漏洞，但是它记录下的入侵信息往往是最真实的。这种蜜罐安装的系统一般都是最初的，没有任何 SP 补丁，或者打了低版本 SP 补丁，根据管理员需要，也可能补上

一些漏洞,只要值得研究的漏洞还存在就必须打补丁。然后把蜜罐连接到网络上,根据目前的网络扫描频繁来看,这样的蜜罐很快就能吸引到目标并接受攻击,系统运行的记录程序会记下入侵者的一举一动,但同时它也是最危险的,因为入侵者每一个入侵都会引起系统真实的反应,例如被溢出、渗透和夺取权限等。

2) 伪系统蜜罐

伪系统也是建立在真实系统基础上的,但是它最大的特点就是“平台与漏洞非对称性”。

大家知道,操作系统不只有 Windows,在这个领域,还有 Linux、UNIX、OS2 和 BeOS 等,它们的核心不同,因此会产生的漏洞和缺陷也就不尽相同,也就是很少有能同时攻击几种系统的漏洞代码,也许用 LSASS 溢出漏洞能拿到 Windows 的权限,但是用同样的手法去溢出 Linux 只能是徒劳的。根据这种特性,能产生“伪系统蜜罐”,它利用一些工具程序强大的模仿能力,伪造出不属于自己平台的“漏洞”,入侵这样的“漏洞”,只能是在一个程序框架里打转,即使成功“渗透”,也仍然是程序制造的梦境——系统本来就没有让这种漏洞成立的条件。实现一个“伪系统”并不困难,Windows 平台下的一些虚拟机程序、Linux 自身的脚本功能加上第三方工具就能轻松实现,甚至在 Linux/UNIX 下还能实时由管理员产生一些根本不存在的“漏洞”,让入侵者自以为得逞。实现跟踪记录也很容易,只要在后台开着相应的记录程序即可。

这种蜜罐的好处在于,能最大程度防止被入侵者破坏,也能模拟不存在的漏洞,甚至可以让一些 Windows 蠕虫攻击 Linux,只要模拟出符合条件的 Windows 特征。但是也存在坏处,因为一个聪明的入侵者只要经过几个回合就会识破伪装,另外,编写脚本并不是一件简单的事情。

5. 蜜罐的用途

既然蜜罐不是做来玩的,管理员自然就不会做个蜜罐然后让它赋闲在家,那么到底怎么用蜜罐呢?

1) 迷惑入侵者,保护服务器

一般的客户机/服务器模式里,浏览者是直接与网站服务器连接的,换句话说,整个网站服务器都暴露在入侵者面前,如果服务器安全措施不够,那么整个网站数据都有可能被入侵者轻易毁灭。但是如果在客户机/服务器模式里嵌入蜜罐,让蜜罐作为服务器角色,真正的网站服务器作为一个内部网络在蜜罐上做网络端口映射,这样可以把网站的安全系数提高,入侵者即使渗透了位于外部的“服务器”,也得不到任何有价值的资料,因为他入侵的是蜜罐而已。虽然入侵者可以在蜜罐的基础上跳进内部网络,但那要比直接攻下一台外部服务器复杂得多,许多水平不足的入侵者只能望而却步。

在这种用途上,蜜罐不能设计得漏洞百出。蜜罐既然成了内部服务器的保护层,就必须要求它自身足够坚固,否则,整个网站都要拱手送人了。

2) 抵御入侵者,加固服务器

入侵与防范一直都是热点问题,而在其间插入一个蜜罐系统将会使防范变得有趣,蜜罐可被设置得与内部网络服务器一样,当一个入侵者费尽力气入侵了这台蜜罐的时

候，管理员已经收集到足够的攻击数据来加固真实的服务器。

采用这个策略去布置蜜罐，需要管理员配合监视，否则入侵者攻破了第一台计算机，就会有第二台计算机受到攻击。

3）诱捕网络罪犯

这是一个相当有趣的应用，当管理员发现一个普通的客户机/服务器模式网站服务器已经牺牲成肉鸡的时候，管理员会迅速修复服务器。那么下次呢？既然入侵者已经确信自己把该服务器做成了肉鸡，他必然还会再次“光临”，可以设置一个蜜罐模拟出已经被入侵的状态，等待黑客的到来。同样，一些企业为了查找恶意入侵者，也会故意设置一些有不明显漏洞的蜜罐，让入侵者在不起疑心的情况下乖乖被记录下一切行动证据，有些人把此戏称为“监狱机”，通过与电信局的配合，可以轻易揪出 IP 源头的那双黑手。

随着网络入侵类型的多样化发展，蜜罐也必须进行多样化的演绎，否则有一天它将无法面对入侵者的肆虐。这也对网络管理员的技术能力有了更高的要求，因为蜜罐是活跃在安全领域的虚拟演员，它的一举一动，都是通过用户自己来设计的。

13.4.3 IP地址侦察和隐藏技术

在正式进行各种“黑客行为”之前，黑客会采取各种手段，探测（也可以说“侦察”）对方的主机信息，以便决定使用何种最有效的方法达到目的。来看看黑客是如何获知最基本的网络信息，如对方的 IP 地址以及用户如何防范自己的 IP 泄漏。

1. 获取 IP 地址

“IP”作为网络用户的重要标识，是黑客首先需要了解的重要信息。获取 IP 的方法较多，黑客也会因不同的网络情况采取不同的方法，如在局域网内使用 ping 命令，ping 对方在网络中的域名而获得 IP；也可在 Internet 上使用 IP 版的 QQ 直接显示，而最最有效的办法是截获并分析对方的网络数据包。可用 Windows 2003 的网络监视器捕获的网络数据包，再通过软件解析截获后的数据包的 IP 包头信息，再根据这些信息了解具体的 IP。

2. 隐藏 IP 地址

虽然侦察 IP 的方法多样，但用户可以隐藏 IP 的方法也很多。就拿对付最有效的“数据包分析方法”而言，就可以安装能够自动去掉发送数据包包头 IP 信息的 Norton Internet Security 2003。不过使用“Norton Internet Security”有些缺点，譬如，它耗费资源严重，降低计算机性能；在访问一些论坛或者网站时会受影响；不适合网吧用户使用等。现在的个人用户采用最普及隐藏 IP 的方法应该是使用代理，由于使用代理服务器后，“转址服务”会对发送出去的数据包有所修改，致使“数据包分析”的方法失效。一些容易泄漏用户 IP 的网络软件（QQ、MSN 和 IE 等）都支持使用代理方式连接 Internet，特别是 QQ 使用 ezProxy 等代理软件连接后，IP 版的 QQ 都无法显示该 IP 地址。还有一款比较适合个人用户的简易代理软件，如“网络新手 IP 隐藏器”，只要在“代理服务器”和“代理服务器端”填入正确的代理服务器地址和端口，即可对 http 使用代理，比较适合由于 IE 和 QQ 泄漏

IP 的情况。

使用代理服务器，同样有一些缺点，比如会影响网络通信的速度；需要网络上的一台能够提供代理能力的计算机；如果用户无法找到这样的代理服务器就不能使用代理（查找代理服务器时，可以使用“代理猎手”等工具软件扫描网络上的代理服务器）。

虽然代理可以有效地隐藏用户 IP，但技术高深的黑客亦可以绕过代理，查找到对方的真实 IP 地址，用户在何种情况下使用何种方法隐藏 IP，也要因情况而论。

习 题 13

1. “黑客”与“入侵者”有何区别？
2. 黑客攻击的基本步骤有哪些？
3. 黑客搜集目标信息的一般步骤有哪些？
4. 什么是拒绝服务攻击？
5. 什么是木马？
6. 常用的木马防范技术有哪些？

附录 A addendum A

缩 略 词 汇

ACL(Access Control List) 访问控制表
ADM(Anomaly Detection Model) 异常检测模型
AH(Authentication Head) 认证头
ARP(Address Resolution Protocol) 地址解析协议
BIOS(Base Input/Output System) 基本输入/输出系统
CA(Certification Authority) 认证中心
CSMA/CD(Carrier Sense Multi-Access/Collision Detection) 载波侦听多路访问/冲突检测
CMOS(Complementary Metal-Oxide-Semiconductor 互补式金属氧化物半导体存储器
CRC(Cyclic Redundancy Check) 循环冗余校验
CPU(Central Processing Unit) 中央控制单元,中央控制器
DAC(Discretionary Access Control) 自主访问控制
DDoS(Distribute Denial of Service) 分布式拒绝服务攻击
DOS(Disk Operation System) 磁盘操作系统
DoS(Denial of Service) 拒绝服务攻击
DZ(Demilitarized Zone) 非军事区域
ECN(Explicit Congestion Notification) 显示拥塞指示算法
ESP(Encapsulating Security Payload) 封装安全净荷
FDDI(Fiber Distributed Data Interface) 光缆分布式数据接口
FIFO(First In First Out) 先进先出算法
FTP(File Transfer Protocol) 文件传输协议
HIDS(Host Intrusion Detect System) 主机入侵检测系统
HSM(Hierarchical Storage Management) 分级存储管理
HTTP(Hyper Text Transfer Protocol) 超文本传输协议
ICMP(Internet Control Message Protocol) 控制报文协议
IDS(Intrusion Detect System) 入侵检测系统
ICV(Integrated Check Vector) 完整性检测向量
IIS(Internet Information Server) Internet 信息服务

IKE(Inter Key Exchange)　Internet 密钥交换协议
IP(Internet Protocol)　网际协议
IPSec(Internet Protocol Security)　因特网安全协议
IPX(Internet Packet eXchange)　网间分组交换
IOS(International Organization for Standardization)　国际标准化组织
MAC(Media Access Control)　介质访问控制
MDM(Misuse Detection Model)　误用检测模型
MIC(Message Integrity Code)　消息完整性编码
NIDS(Network Intrusion Detect System)　网络入侵检测系统
OSI(Open System Interconnection)　开放系统互连参考模型
PDA(Personal Digital Assistant)　个人数字助理
PKI(Public Key Infrastructures)　公钥基础设施
QoS(Quality of Service)　服务质量
RAID(Redundant Arrays of Independent Disks)　磁盘阵列
RARP(Reverse Address Resolution Protocol)　反向地址解析协议
RBAC (Role Based Access Conto1)　基于角色的访问控制模式
RED(Random Early Detection)　随机早期检测算法
SMTP(Simple Mail Transfer Protocol)　简单邮件传输协议
SPI(Security Parameter Index)　安全参数索引
SSL(Secure Socket Layer)　安全套接字层
TCB(Trusted Computing Base)　可信计算基础
TCP(Transmission Control Protocol)　传输控制协议
TCP/IP(Transmission Control Protocol/Internet Protocol)　Internet 协议簇
UDP(User Datagram Protocol)　用户报文协议

参 考 文 献

1 杨云江主编. 计算机网络基础. 北京：清华大学出版社，2004
2 杨云江编著. 计算机网络管理技术. 北京：清华大学出版社，2005
3 Dieter Gollmann. Computer Security. The edition published by John Wiley & Sons，Ltd. 1999
4 段云所等编著. 信息安全概论. 北京：高等教育出版社，2003
5 蔡皖东编著. 网络与信息安全. 西安：西北工业大学出版社，2004
6 Amato V 编著. 思科网络技术学院教程. 韩江，马刚译. 北京：人民邮电出版社，2002
7 彭澎编著. 计算机网络实用教程. 北京：电子工业出版社，2000
8 Comer D E 著. 用 TCP/IP 进行国际互联. 林瑶等译. 北京：电子工业出版社，2001
9 叶忠杰等编著. 计算机网络安全技术. 北京：科学出版社，2003
10 Maiwald E 著. 网络安全实用教程. 李庆荣等译. 北京：清华大学出版社，2003
11 戚文静等编著. 网络安全与管理. 北京：中国水利水电出版社，2003
12 凌雨欣等编著. 网络安全技术与反黑客. 北京：冶金工业出版社，2001
13 袁家政等编著. 计算机网络安全与应用技术. 北京：清华大学出版社，2002
14 葛秀慧等编著. 计算机网络安全管理. 北京：清华大学出版社，2003
15 林涛主编. 网络安全与管理. 北京：电子工业出版社，2005
16 胡道元，闵京华编著. 网络安全. 北京：清华大学出版社，2005
17 刘建伟，王育民编著. 网络安全——技术与实践. 北京：清华大学出版社，2005
18 罗斌，郭峥嵘编著. 网络安全设计标准. 北京：清华大学出版社，2005
19 张新有主编. 网络工程技术与实践教程. 北京：清华大学出版社，2005
20 兰少华等编著. TCP/IP 网络与协议. 北京：清华大学出版社，2006
21 陈向阳等编著. 计算机网络与通信. 北京：清华大学出版社，2005
22 唐正军，李建华编著. 入侵检测技术. 北京：清华大学出版社，2004
23 阙喜戌等编著. 信息安全原理及应用. 北京：清华大学出版社，2003
24 卿斯汉编著. 安全协议. 北京：清华大学出版社，2005
25 张玉清等编著. 安全扫描技术. 北京：清华大学出版社，2004
26 余建伟等编著. 防守反击：黑客攻击手段分析与防范. 北京：人民邮电出版社，2001

高等院校信息技术规划教材

系 列 书 目

书　　名	书　号	作　者
数字电路逻辑设计	978-7-302-12235-7	朱正伟　等
计算机网络基础	978-7-302-12236-4	符彦惟　等
微机接口与应用	978-7-302-12234-0	王正洪　等
XML 应用教程(第 2 版)	978-7-302-14886-9	吴　洁
算法与数据结构	978-7-302-11865-7	宁正元　等
算法与数据结构习题精解和实验指导	978-7-302-14803-6	宁正元　等
工业组态软件实用技术	978-7-302-11500-7	龚运新　等
MATLAB 语言及其在电子信息工程中的应用	978-7-302-10347-9	王洪元
微型计算机组装与系统维护	978-7-302-09826-3	厉荣卫　等
嵌入式系统设计原理及应用	978-7-302-09638-2	符意德
C++语言程序设计	978-7-302-09636-8	袁启昌　等
计算机信息技术教程	978-7-302-09961-1	唐全　等
计算机信息技术实验教程	978-7-302-12416-0	唐全　等
Visual Basic 程序设计	978-7-302-13602-6	白康生　等
单片机 C 语言开发技术	978-7-302-13508-1	龚运新
ATMEL 新型 AT89S52 系列单片机及其应用	978-7-302-09460-8	孙育才
计算机信息技术基础	978-7-302-10761-3	沈孟涛
计算机信息技术基础实验	978-7-302-13889-1	沈孟涛　著
C 语言程序设计	978-7-302-11103-0	徐连信
C 语言程序设计习题解答与实验指导	978-7-302-11102-3	徐连信　等
计算机组成原理实用教程	978-7-302-13509-8	王万生
微机原理与汇编语言实用教程	978-7-302-13417-6	方立友
微机组装与维护用教程	978-7-302-13550-0	徐世宏
计算机网络技术及应用	978-7-302-14612-4	沈鑫剡　等
微型计算机原理与接口技术	978-7-302-14195-2	孙力娟　等
基于 MATLAB 的计算机图形与动画技术	978-7-302-14954-5	于万波
基于 MATLAB 的信号与系统实验指导	978-7-302-15251-4	甘俊英
信号与系统学习指导和习题解析	978-7-302-15191-3	甘俊英
计算机与网络安全实用技术	978-7-302-15174-6	杨云江

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室　收
邮编：100084　　　　电子邮件：jsjjc@tup.tsinghua.edu.cn
电话：010-62770175-4608/4409　　　　邮购电话：010-62786544

教材名称：计算机与网络安全实用技术

ISBN：978-7-302-15174-6

个人资料

姓名：__________ 年龄：______ 所在院校/专业：______________

文化程度：__________ 通信地址：______________________

联系电话：__________ 电子信箱：______________________

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议______________

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议______________

您对本书的总体满意度：

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

____

____

您希望本书在哪些方面进行改进？（可附页）

____

____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。